IAS
WINTER
SCHOOL
2026

AI4I / CSP
IAS \ INSTITUTE
FOR ADVANCED
STUDY

AI4I
AI FOR INDUSTRY
The Italian Institute of
Artificial Intelligence

Fondazione
Compagnia
di San Paolo

CRYPTOGRAPHY AND MACHINE LEARNING

PROGRAM

Winter School on Machine Cryptography and Machine Learning

ORGANIZED BY	BASIC INFORMATION	
Valerio Cini **Giulio Malavolta** **Tamer Mour** **Emmanuela Orsini** **Alon Rosen** (Bocconi, Milan, Italy)	Name of the School:	**CSP – IAS – Winter School**
	Organizing institutions:	**CSP – IAS – the Institute for Advanced Study of AI4I** WEB ↗
	Dates:	**February 2–5, 2026**
	Venue:	OGR - Officine Grandi Riparazioni WEB ↗ Corso Castelfidardo, 22, Turin, Italy MAP ↗

TOPIC OF THE SCHOOL

The school will cover the main areas of this field (together with the necessary mathematical background):

- Primers on cryptography and machine learning: Introductory lectures providing a common foundation for participants from different backgrounds.
- Backdoors in machine learning models: Understanding how hidden or malicious functionality can be introduced into models during training or deployment, and studying cryptographic methods for detection and prevention.
- Adversarial machine learning: Exploring attacks that exploit model vulnerabilities through carefully crafted inputs, and developing defenses that improve robustness and reliability.
- Model integrity and verifiability: Techniques ensuring that trained models and their outputs can be authenticated, verified, and trusted.
- Cryptanalysis techniques tailored to machine learning systems: How ideas and methodologies from cryptanalysis and theoretical cryptography can be adapted to study vulnerabilities, leakage, and robustness in learning-based systems.
- Watermarking and methods for tracing and verifying AI-generated content: Cryptographic and algorithmic techniques to enable attribution and detection of outputs of learning models.
- Average-case hardness and its connection to secure ML constructions: Theoretical aspects linking computational hardness assumptions with the design of secure machine learning models.

IAS CRYPTOGRAPHY
WINTER AND MACHINE
SCHOOL LEARNING
2026 TURIN / FEBRUARY 2-5

IAS
AI4I / CSP
IAS \ INSTITUTE
FOR ADVANCED
STUDY

AI4I
AI FOR INDUSTRY
The Italian Institute of
Artificial Intelligence

Fondazione
Compagnia
di San Paolo

Program

	Monday 02	Tuesday 03	Wednesday 04	Thursday 05
9:00 - 9:30	*Coffee*			
9:30 - 11:00	Primer Cryptography for machine Learners	Watermarking	Backdoors	Security and Cryptanalysis
11:00 - 11:30	*Coffee*			
11:30 - 13:00	Primer Cryptography for machine Learners	Integrity	Cryptography Hardness in Learning	Adversarial ML
13:00 - 14:30	*Lunch*			
14:30 - 15:15	Keynote	Keynote	Excursion	Keynote
15:15 - 16:00	Primer Cryptography for machine Learners	Panel New Directions		Panel
16:00 - 16:30	*Coffee*			
16:30 - 17:15	Unstructured time for discussion	Unstructured time for discussion		

am outlined above is tentative;
some sessions may be rearranged depending on the final availability of the speakers.