

IASWIS  
IAS  
WINTER  
SCHOOL  
2026

IAS  
AI4I / CSP  
IAS \ INSTITUTE  
FOR ADVANCED  
STUDY

AI<sup>4</sup>I  
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	
<b>Valerio Cini</b> <b>Giulio Malavolta</b> <b>Tamer Mour</b> <b>Emmanuela Orsini</b> <b>Alon Rosen</b>  (Bocconi, Milan, Italy)	Name of the School:	<b>CSP - IAS - Winter School</b>
	Organizing institutions:	<b>CSP - IAS - the Institute for Advanced Study of AI4I</b> <a href="#">WEB</a> ↗
	Dates:	<b>February 2-5, 2026</b>
	Venue:	OGR - Officine Grandi Riparazioni <a href="#">WEB</a> ↗ Corso Castelfidardo, 22, Turin, Italy <a href="#">MAP</a> ↗

IN COOPERATION WITH IACR AND THE DEPARTMENT OF COMPUTING SCIENCES AT BOCCONI UNIVERSITY

### 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.

## FACULTY

### **Luca Biggio**

*Assistant Professor, Department of Computing Sciences, Bocconi University*

### **Valerio Cini**

*Marie Skłodowska-Curie Postdoctoral Fellow, Bocconi University*

### **Miranda Christ**

*PhD Student, Columbia University*

### **Dario Fiore**

*Associate Research Professor, IMDEA*

### **Nicola Franco**

*Director, AI Security R&D Lab, AI4I*

### **Rosario Gennaro**

*Distinguished Professor of Computer Science, Director of CAISS, The City College of New York*

### **Sanjam Garg**

*Associate Professor, University of California, Berkeley*

### **Tal Herman**

*Simons-Berkeley Postdoctoral Researcher, MIT*

### **Marc Mézard**

*Professor of Theoretical Physics, Bocconi University*

### **Odelia Melamed**

*PhD Student, Weizmann Institute of Science*

### **Shay Moran**

*Associate Professor, Departments of Mathematics, Computer Science, and Data and Decision Sciences, Technion*

### **Tamer Mour**

*Postdoctoral Researcher, Bocconi University*

### **Adi Shamir**

*Paul and Marlene Borman Professorial Chair of Applied Mathematics, Weizmann Institute of Science*

### **Mahmood Sharif**

*Senior Lecturer, Blavatnik School of Computer Science, Tel Aviv University*

### **Neekon Vafa**

*PhD Student, MIT*

### **Daniele Venturi**

*Full Professor, Computer Science Department, Sapienza University of Rome*

### **Vinod Vaikuntanathan**

*Ford Foundation Professor of Engineering (EECS), MIT; Principal Investigator, CSAIL MIT; Chief Cryptographer, Duality Technologies*

### **Or Zamir**

*Senior Lecturer, Blavatnik School of Computer Science, Tel Aviv University*

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



Program	Monday 02	Tuesday 03	Wednesday 04	Thursday 05
9:00 - 9:30	Welcome Remarks <b>Fabio Pammolli</b> <i>President, The Italian Institute of Artificial Intelligence (AI4I)</i>	Coffee	Coffee	Coffee
9:30 - 10:15	Cryptography for machine Learners <b>Valerio Cini</b> <i>Marie Skłodowska-Curie Postdoctoral Fellow, Bocconi University</i>	Misuse-Resistant Machine Learning <b>Sanjam Garg</b> <i>Associate Professor, University of California, Berkeley</i>	Machine Unlearning <b>Odelia Melamed</b> <i>PhD student, Weizmann Institute of Science</i>	Watermarking: Impossibility <b>Daniele Venturi</b> <i>Full Professor at the Computer Science Department, Sapienza University of Rome</i>
10:15 - 11:00	Cryptography for machine Learners <b>Tamer Mour</b> <i>Postdoctoral Researcher at Bocconi University</i>	Verifiable Data Science <b>Tal Herman</b> <i>Simons-Berkeley postdoctoral researcher MIT</i>	Adversarial ML <b>Mahmood Sharif</b> <i>Senior Lecturer, Blavatnik School of Computer Science at Tel Aviv University</i>	Watermarking: Constructions <b>Miranda Christ</b> <i>PhD student, Columbia University</i>
11:00 - 11:30	Coffee			
11:30 - 12:15	Machine Learning for Cryptographers <b>Shay Moran</b> <i>Associate Professor, Departments of Mathematics, Computer Science, and Data and Decision Sciences, Technion</i>	Modular Sumcheck Proofs for Private ML <b>Dario Fiore</b> <i>Associate Research Professor, IMDEA</i>	Formal Cryptographic Guarantees in ML I/II <b>Or Zamir</b> <i>Senior Lecturer, Blavatnik School of Computer Science at Tel Aviv University</i>	Cryptographic Hardness in Learning I <b>Neekon Vafa</b>
12:15 - 13:00		Towards Lightweight Verifiable AI <b>Rosario Gennaro</b> <i>Distinguished Professor of Computer Science, Director of CAISS, The City College of New York</i>		Cryptographic Hardness in Learning II <b>Neekon Vafa</b> <i>PhD Student, MIT</i>
13:00 - 14:30	Break			
14:30 - 15:15	Keynote: Generative Diffusion <b>Marc Mézard</b> <i>Professor of Theoretical Physics at Bocconi University</i>	Cryptography and AI <b>Vinod Vaikuntanathan</b> <i>Ford Foundation Professor of Engineering EECS MIT, principal investigator CSAIL MIT, chief cryptographer Duality Technologies</i>	Excursion	Keynote: Deep Neural Cryptography <b>Adi Shamir</b> <i>Paul and Marlene Borman Professorial Chair of Applied Mathematics at Weizmann Institute of Science</i>
15:15 - 16:00	Machine Learning for Cryptographers <b>Luca Biggio</b>	Panel		Closing Remarks <b>Alon Rosen</b> <i>Professor, Bocconi University</i>
16:00 - 16:30	Coffee			Coffee
16:30 - 17:15	Machine Learning for Cryptographers <b>Luca Biggio</b> <i>Assistant Professor, Department of Computing Sciences at Bocconi University</i>	Adversarial Robustness in Quantum Machine Learning <b>Nicola Franco</b> <i>Director AI Security R&amp;D Lab, AI4I</i>		Unstructured time for discussion
17:15 - 18:00	-			-