Dagstuhl Seminar 26401 · Divided We Stand: Security and Privacy of Collaborative Learning

28 September – 2 October 2026 · Schloss Dagstuhl

https://www.dagstuhl.de/26401

Monday, 28 September 2026			
Time	**Activity / Session**	**Speaker**	**Talk title / Details**
09:00–09:10	Organizers' introduction	**Organizers**	
09:10–10:30	Participant introductions	**Participants**	Approximately 2 minutes per participant
10:30–11:00	*Coffee break*	-	
11:00–12:00	Seminar topics and programme overview	**Antonino Nocera**	
12:00–13:00	*Lunch*	-	
	Session 1 · Cryptographic Foundations for Privacy-Preserving Collaborative Learning		
13:15–13:30	Talk	**Olena Ivanova**	Homomorphic Encryption Schemes for Collaborative Learning or Collaborative Inference
13:30–13:45	Talk	**Christian Weinert**	Multi-Party Computation for Secure and Private Collaborative Training and Federated Learning
13:45–14:00	Talk	**Antonia Sophie Boy**	Cryptographic Mechanisms for Securing Federated Learning
14:00–15:00	Plenary discussion	-	
15:00–16:00	*Cake break*	-	
16:00–17:30	Breakout sessions	-	

Tuesday, 29 September 2026			
Time	**Activity / Session**	**Speaker**	**Talk title / Details**
	Session 2 · Emerging Privacy Risks and Security Boundaries in Collaborative Learning		
09:15–09:30	Talk	**Vasisht Duddu**	Unintended Interactions and Opportunities in Collaborative Learning
09:30–09:45	Talk	**Marco Arazzi**	Beyond the Server: The Missing Participant-Side Adversary in Federated Learning Privacy
09:45–10:00	Talk	**Nikhilesh Kumar Singh**	When Collaboration Moves to Inference: New Security Boundaries in LLM Serving
10:00–11:00	*Coffee break*	-	
11:00–12:00	Plenary discussion	-	
12:00–13:00	*Lunch*	-	
	Session 3 · Privacy and Robustness: Tensions, Monitoring, and Co-Design		
13:00–13:15	Talk	**Sayan Biswas**	Building Neighborhoods That Keep Secrets and Catch Trojans: Privacy and Robustness Native to Decentralized ML
13:15–13:30	Talk	**Fatih Turkmen**	Fully Decentralized Learning with Privacy Guarantees and Byzantine Robustness
13:30–13:45	Talk	**Phillip Rieger**	Split Learning for LLMs: How Can We Protect Privacy While Enabling Monitoring?
13:45–14:00	Talk	**Jérémie Decouchant**	Beyond the Idealized Setting: System Realities vs. Robustness and Privacy
14:00–15:00	Plenary discussion	-	
15:00–16:00	*Cake break*	-	
16:00–17:30	Breakout sessions	-	

Wednesday, 30 September 2026			
Time	**Activity / Session**	**Speaker**	**Talk title / Details**
	Session 4 · Attack Vectors and Vulnerabilities in Collaborative Learning		
09:15–09:30	Talk	**Alessandro Pegoraro**	The Implicit Negotiations in Collaborative Learning
09:30–09:45	Talk	**Aliza Reif**	An Attack On Modality Prioritization For Multimodal Sensor Fusion
09:45–10:00	Talk	**Alexandra Dmitrienko**	Beyond Honest-but-Curious: Memory Backdoors in Collaborative Learning
10:00–11:00	*Coffee break*	-	
11:00–12:00	Plenary discussion	-	
12:00–13:00	*Lunch*	-	
13:00–17:30	Social activity	-	

Thursday, 1 October 2026			
Time	**Activity / Session**	**Speaker**	**Talk title / Details**
	Session 5 · Applications, Agency, and Accountability in Collaborative Learning		
09:15–09:30	Talk	**Giovanni Apruzzese**	Can We Use Federated Learning to Fight Phishing?
09:30–09:45	Talk	**Janani Kehelwala**	Decentralized Agency for Collaborative Security in Future Networks
09:45–10:00	Talk	**Lydia Y. Chen**	Watermarking Structured Data
10:00–11:00	*Coffee break*	-	
11:00–12:00	Plenary discussion	-	

Dagstuhl Seminar 26401 · Divided We Stand: Security and Privacy of Collaborative Learning

28 September – 2 October 2026 · Schloss Dagstuhl

https://www.dagstuhl.de/26401

12:00–13:00	*Lunch*	-	
	Session 6 · Attacks, Model Manipulation, and Robust Defenses		
13:00–13:15	Talk	**Oguzhan Ersoy**	Attacks and Defenses in Decentralized Collaborative Learning: New Directions in the LLM Era
13:15–13:30	Talk	**Lichao Wu**	Inside the Model: LLM Neuron Editing for Good and Evil
13:30–13:45	Talk	**Gianluca Lax**	From Rejection to Auditing: Managing Anomalous Updates of the Global Model
13:45–14:00	Talk	**Marco Arazzi**	Robust Aggregation in Federated LoRA
14:00–15:00	Plenary discussion	-	
15:00–16:00	*Cake break*	-	
16:00–17:30	Breakout sessions and preparation for final synthesis	-	

Friday, 2 October 2026

Time	Activity / Session	Speaker	Talk title / Details
09:15–10:30	Seminar synthesis	-	Key findings and open research questions
10:30–11:00	*Coffee break*	-	
11:00–11:45	Follow-up activities and collaboration planning	-	
11:45–12:00	Closing remarks	**Organizers**	
12:00–13:00	*Lunch and departure*	-	