Universität Münster

FACHBEREICH 10
MATHEMATIK UND INFORMATIK
Prof. Dr. Arthur Bartels
Dekan

20.01.2026

Einladung

zu der am Mittwoch, den 28. Januar 2026,
um 11:15 Uhr im Hörsaal M4 stattfindenden

Antrittsvorlesung

von Herrn Prof. Dr. Zoltán Mann

über das Thema

„Sicheres maschinelles Lernen und andere Illusionen“

Kurzfassung:
Maschinelles Lernen (ML) findet in immer mehr Bereichen Anwendung, darunter zunehmend auch auf sicherheitskritischen Gebieten, wie autonomes Fahren oder medizinische Diagnose und Therapie. Damit wachsen auch die Sicherheitsbedenken. Dieser Vortrag gibt einen Überblick über einige der gewünschten Sicherheitseigenschaften von ML und inwiefern diese Eigenschaften bei gängigen ML-Verfahren gegeben sind. Im zweiten Teil des Vortrags wird anhand des Beispiels der datenschutzfreundlichen Inferenz mit neuronalen Netzen aufgezeigt, wie gewisse Sicherheitseigenschaften mit kryptografischen Methoden garantiert werden können und welchen Preis man dafür zahlen muss.

gez. Arthur Bartels, Dekan