

## **Antonio Emanuele Cinà (Cv)**

**Bio:** Antonio Emanuele Cinà is an Assistant Professor (RTDA) in Computer Science at the University of Genoa, Italy, since June 2023. He earned his Ph.D. cum laude from Ca' Foscari University of Venice in 2023, where his doctoral work focused on the vulnerabilities and emerging threats arising from the malicious manipulation of training data in AI systems. His work sits at the intersection of artificial intelligence and security, with core expertise in training-time (poisoning) and inference-time (evasion) attacks. Antonio's research aims to uncover and address the risks that undermine the availability, reliability and trustworthiness of modern AI. More recently, Antonio has been exploring how Generative AI (LLMs) can be leveraged to advance cybersecurity, bridging the gap between offensive strategies and robust defense mechanisms.