Roma Tre

Dipartimento di Matematica e Fisica
Segreteria per la Ricerca

italian

SEMINARIO di CRITTOGRAFIA

Massimiliano SALA

(Università di Trento)

Una chat privata con l'AI

28 Maggio 2026

ore 15.00

Largo San Leonardo Murialdo 1 - Edificio C

AULA C309

Abstract: Utilizzare modelli come **ChatGPT** è senza dubbio comodo, ma rischia di esporre i nostri prompt (e i risultati degli stessi). Ad esempio, se un ricercatore avesse un'idea di un possibile brevetto e chiedesse una valutazione a un modello online, potrebbe trovarsi con l'idea rubata da qualcun altro. Oppure se si facessero domande che sottintendono gravi problemi di salute o situazioni di disagio, ci si potrebbe trovare con conseguenze impreviste e spiacevoli. Per ovviare a tutto ciò, alcuni ricercatori hanno sviluppato **Palliora** e **Valorae**. **Palliora** è una piattaforma, basata su tecnologia blockchain e su protocolli decentralizzati, che permette calcoli confidenziali. **Valorae** è una dApp di **Palliora** e permette di interrogare dei modelli LLM in maniera totalmente privata: nessuno (a parte l'utente) vede né il prompt inserito né i risultati, nessuno potrà nemmeno in futuro ricostruirli. La sicurezza di **Valorae** si basa su una combinazione di sicurezza matematica (crittografia) e hardware (TEE).

per informazioni: Dr. Nicoletta Falcone (nicoletta.falcone@uniroma3.it)