Contribution ID: **60** Type: **not specified**

Collision Resistance in random Neural Network-Based Hash Functions

Monday 23 September 2024 14:30 (50 minutes)

Contemporary post-quantum cryptographic protocols rely on worst-case intractability assumptions and consist of multiple intricate steps. In contrast, in this talk we shall explore a model system that directly addresses fundamental computational challenges and that can be mapped on a random neural networks.

We investigate the collision resistance property of a specific class of neural networks, positing that it is difficult to find two distinct sets of weights that produce the same labels for a random data set. Our analysis demonstrates this by upper bounding the local entropy as a function of the distance between collision pairs, revealing the emergence of an overlap gap property—a phenomenon widely considered a significant obstacle for efficient algorithms, including quantum annealing. These theoretical results are corroborated by numerical experiments employing approximate message passing algorithms and simulated annealing, both of which fail well before the predicted thresholds. Our findings suggest potential applications in contemporary cryptography, where these neural networks can be utilized to develop secure cryptographic hash functions.

Presenter: Prof. ZECCHINA, Riccardo (Università Bocconi)

Session Classification: Keynotes