

Bombelli Theory Day: Challenges and Recent Advances in Cryptography

When: December 14th 2023.

Where: Kelsen Room in Palazzo Gaudenzi (Bologna).

10:30 - 10:45	Opening Remarks
10:45 - 11:30	Emmanuela Orsini: “The FAEST Digital Signature Algorithm”
10:30 - 12:15	Tamer Mour: “On The Black-Box Complexity of Correlation Intractability”
12:15 - 14:00	Lunch Break
14:00 - 14:45	Nikolaj Schwartzbach: “k-SUM in the Sparse Regime”
14:45 - 15:30	Pedro Branco: “Traitor Tracing without a Trusted Authority”
15:30 - 17:00	Open Discussion

All times are in Italian time (CET).