# Security of Sparse BullShark and variations (M1)

- Advisor: Petr Kuznetsov
- Location: Telecom building, Palaiseau

A recent approach to building consensus protocols on top of Directed Acyclic Graphs (DAGs) shows much promise due to its simplicity and stable throughput. However, as each node in the DAG typically includes a linear number of references to the nodes in the previous round, prior DAG protocols only scale up to a certain point when the overhead of maintaining the graph becomes the bottleneck. In a recently proposed *sparse* DAG architecture, each node includes only a constant number of references to random nodes in the previous round. The proposal shows a lot of promise in practice, but lacks formal specification and security proofs.

For students interested in scalable distributed systems and cryptographic tools.

## References:


- DAG-Rider: https://arxiv.org/abs/2102.08325
- Bullshark: https://arxiv.org/abs/2201.05677, https://arxiv.org/abs/2209.05633
- Sparse Bullshark: https://arxiv.org/abs/2506.13998