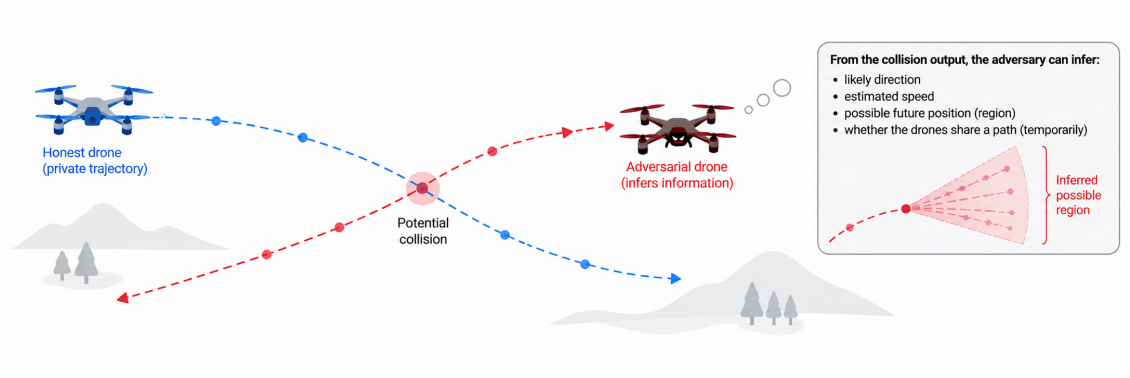
Secure Computation, Insecure Output? Privacy Leakage from Collision Detection



Privacy-preserving trajectory matching allows two autonomous systems to detect potential collisions without revealing their complete trajectories. Modern approaches use secure computation techniques so that the protocol itself reveals nothing beyond its prescribed output. However, this raises an important question: how private is the output itself? In particular, some trajectory-matching constructions reconstruct the collision result for every pair of trajectory points, effectively revealing a collision pattern or matrix rather than a single yes/no answer. A sequence of such outputs may expose much more than the individual collision locations: an adversary may infer whether two vehicles follow the same route, estimate local direction or speed, or narrow down the possible region of future trajectory points.

This project will investigate output-leakage attacks against privacy-preserving trajectory-matching protocols. Different disclosure patterns will be considered, including a single collision, consecutive collisions, alternating or random collisions, and multiple collision bursts separated by gaps. The project can combine analytical leakage models with Monte Carlo-style experiments in which candidate trajectories are generated or sampled and an attacker attempts to infer hidden or future positions from the observed collision pattern. The resulting attacks will then motivate alternative output functionalities. For example, selectively revealing information required for collision avoidance and investigate how these mitigations can be implemented securely.

The student will:

- Model the leakage and different scenarios, characterising how different collision-output patterns reduce uncertainty about a private trajectory.
- Model and evaluate attacks, exploring inference strategies and measuring their success rate under different trajectory, sampling, and disclosure scenarios.
- Propose mitigations, studying what information should be revealed instead of a complete collision matrix and how such restricted outputs can be realised efficiently within privacy-preserving protocols.

Practicalities

Promotor:	Bart Preneel		
Daily supervisor:	Dominik Roy George	dgeorge@esat.kuleuven.be	office B01.24
	Martin Zbudila	martin.zbudila@esat.kuleuven.be	office B01.19
Nature of the work:	25% literature, 25% theoretical work, 50% implementation		
Number of students:	1		

 © 2026 – 2027 COSIC