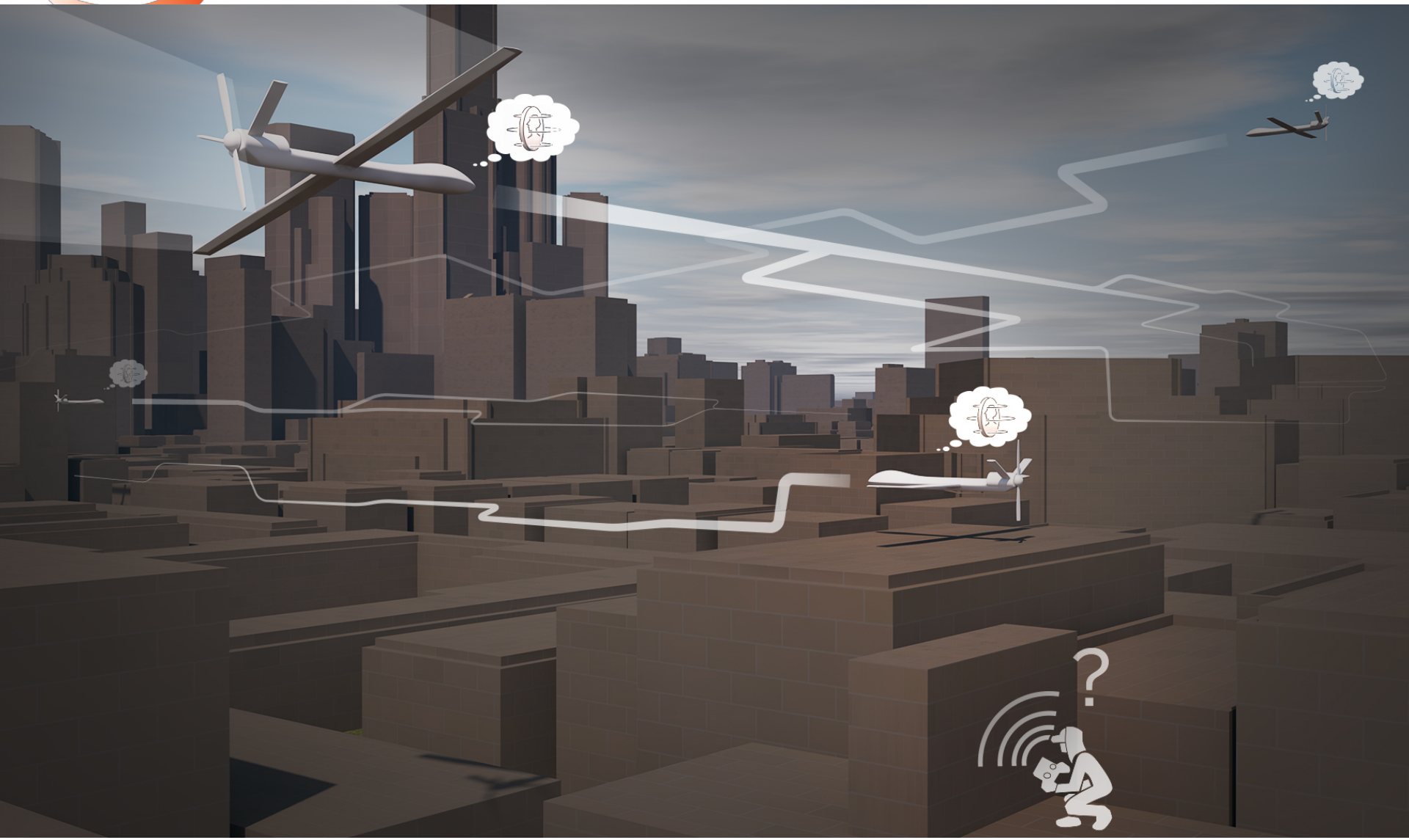
# Protecting safety- and mission-critical information




UF UNIVERSITY of FLORIDA

Duke UNIVERSITY

TEXAS The University of Texas at Austin

UC SANTA CRUZ

# Protecting privacy in computing

- Privacy-preserving computing using secure multiparty computation
  - Semi-honest vs malicious models
- Outsourcing computation to third-parties while maintaining security
- Trustworthy platform architectures and SMC

UF UNIVERSITY of FLORIDA  Duke UNIVERSITY  TEXAS The University of Texas at Austin  UC SANTA CRUZ

# Protecting privacy in communication

- Coalitions can require agents to share sensitive information, such as locations
- Agents must protect information as it is being shared
- Differential privacy provides a statistical privacy framework that we can leverage to safeguard data in communications

# Protecting privacy in execution

- Privacy in terms of evolution of beliefs of an agent or an intruder
- Verification of privacy properties as optimization-based search of algebraic certificates