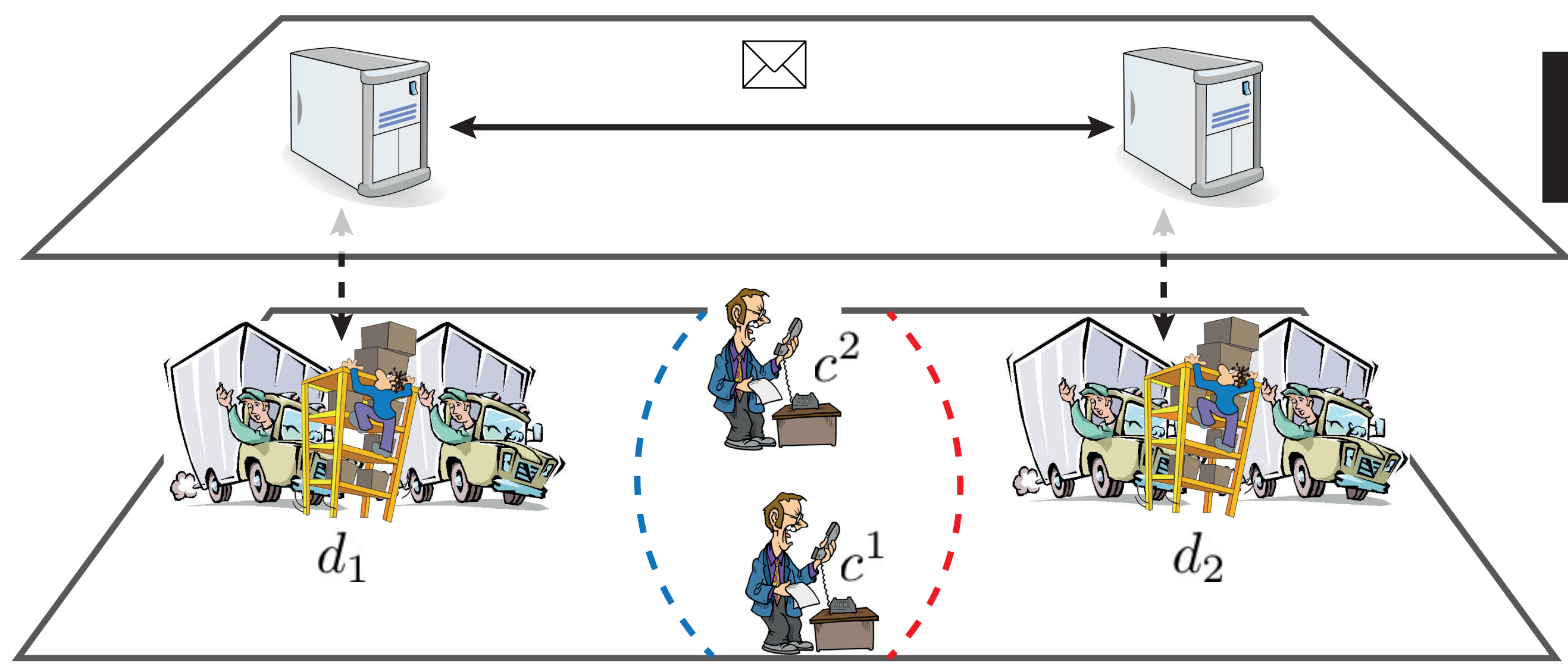


Coordinating Logistics Operations with Privacy Guarantees



Multi-agent Vehicle Routing



Objective: serve all customers at minimum total route length

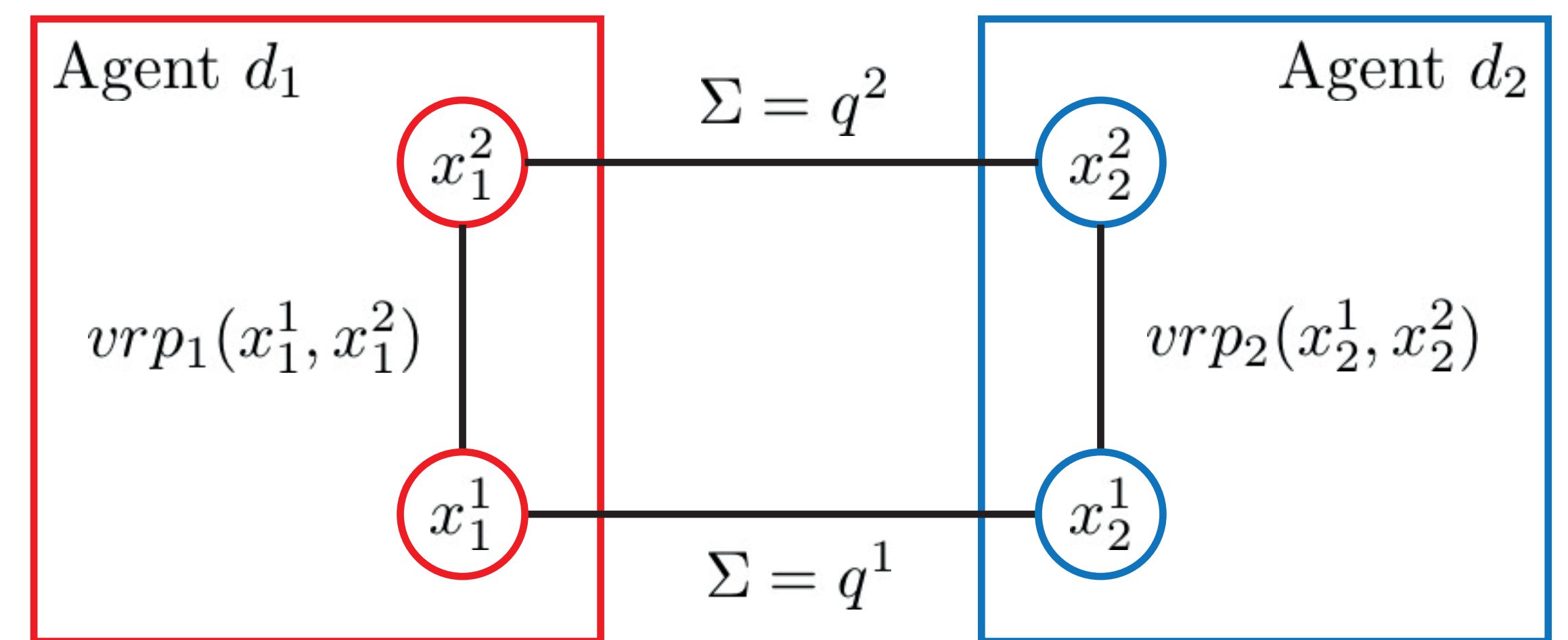
Multi-agent, Master Problem:

- Split customer demands among the depot(s) in reach
- Requires the exchange of messages for depots to coordinate

Local, Slave Problems:

- Each depot must plan vehicle routes to serve its assigned customers
- Depots want to protect the knowledge of their respective local problems

Distributed Constraint Optimization



DCOP Definition:

- A set of agents
- A set of variables
- A set of domains for the variables
- A set of constraints

Objective: assign a value to each variable that minimizes the sum of the costs

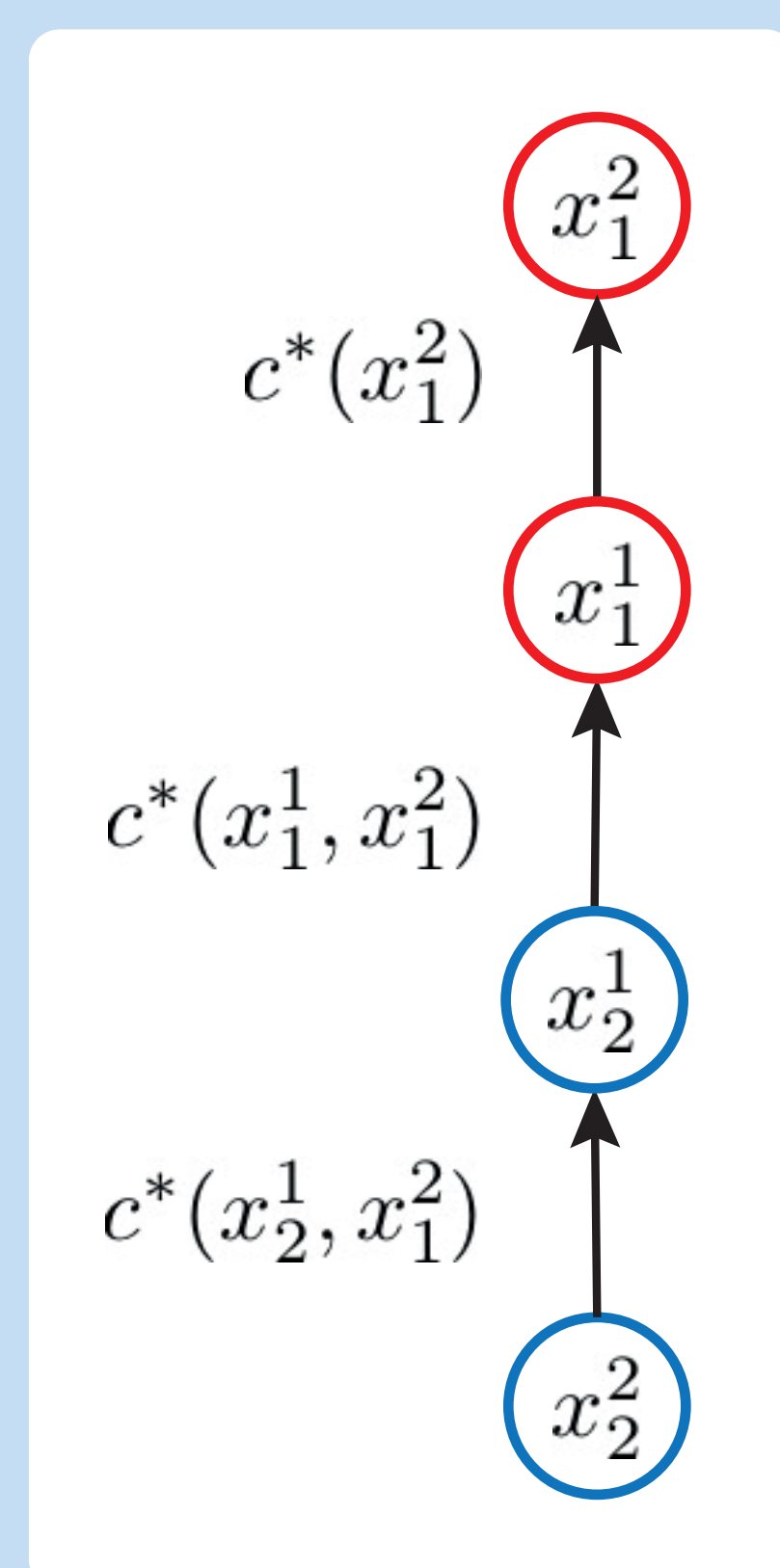
VRP as a DCOP:

- **Agents:** the depots; customers do not participate in the algorithm
- **Variables:** how much of a given customer's demand is served by a given depot
- **Constraints:** SUM constraints + VRP constraints

Privacy through Distributed Computation

P-DPOP

- 1) **Anonymous variable election:** using the viral propagation of random variable scores, the agents elect one variable as the *root*. Only the agent owning the elected variable discovers which is the root.
- 2) **Pseudo-tree generation:** variables are ordered along a pseudo-tree, using a distributed traversal of the constraint graph
- 3) **UTIL propagation:** using distributed dynamic programming, the agents compute the optimal aggregated costs of their respective sub-trees. Variable names a hidden using secret codenames, and costs are obfuscated by adding secret, large, random numbers
- 4) **VALUE propagation:** optimal values to variables are sent top-down, hidden using secret codenames



P^{3/2}-DPOP

- Instead of performing VALUE propagation, which leaks the optimal values of neighboring variables, **the pseudo-tree is re-rooted, and UTIL propagation is performed n times**, with each of the n variables at the root once it turn

P²-DPOP

- Instead of just adding large, random numbers, costs are encrypted using **ElGamal homomorphic encryption**
- Because ElGamal is only *partially* homomorphic, variables must be ordered along a **linear ordering** instead of a pseudo-tree
- A **secure message routing protocol** allows variables to exchanges messages along the linear order without knowing the full topology

Previous Work:

MPC-DisWCSP4 [Silaghi, 2005]

- Requires secure **pair-wise communication** between all agents
- **Agents must agree on an ordered list of candidate solutions**; each agent then expresses its private constraints as a cost vector indexed by the candidate solutions
- **Shamir secret sharing**: each agent gets a *share* of each other agent's secret vector
- **Paillier homomorphic encryption**: vector shares are encrypted and randomly permuted using a **mix-net** in order to eventually produce a randomly chosen optimal solution
- **Iterative algorithm**: agents look for a solution of increasing cost, starting from zero
- **Arithmetic circuits** are used at each iteration to find the first solution of current cost in the randomly permuted list of candidate solutions
- The optimal value of each variable is only revealed to its owner agent

Privacy Properties

privacy:	agent	topology	constraint	decision
P2-DPOP	++	+	++	++
P3/2-DPOP	++	+	+	++
P-DPOP	++	+	+	+
MPC-DisWCSP4	-	-	+	+

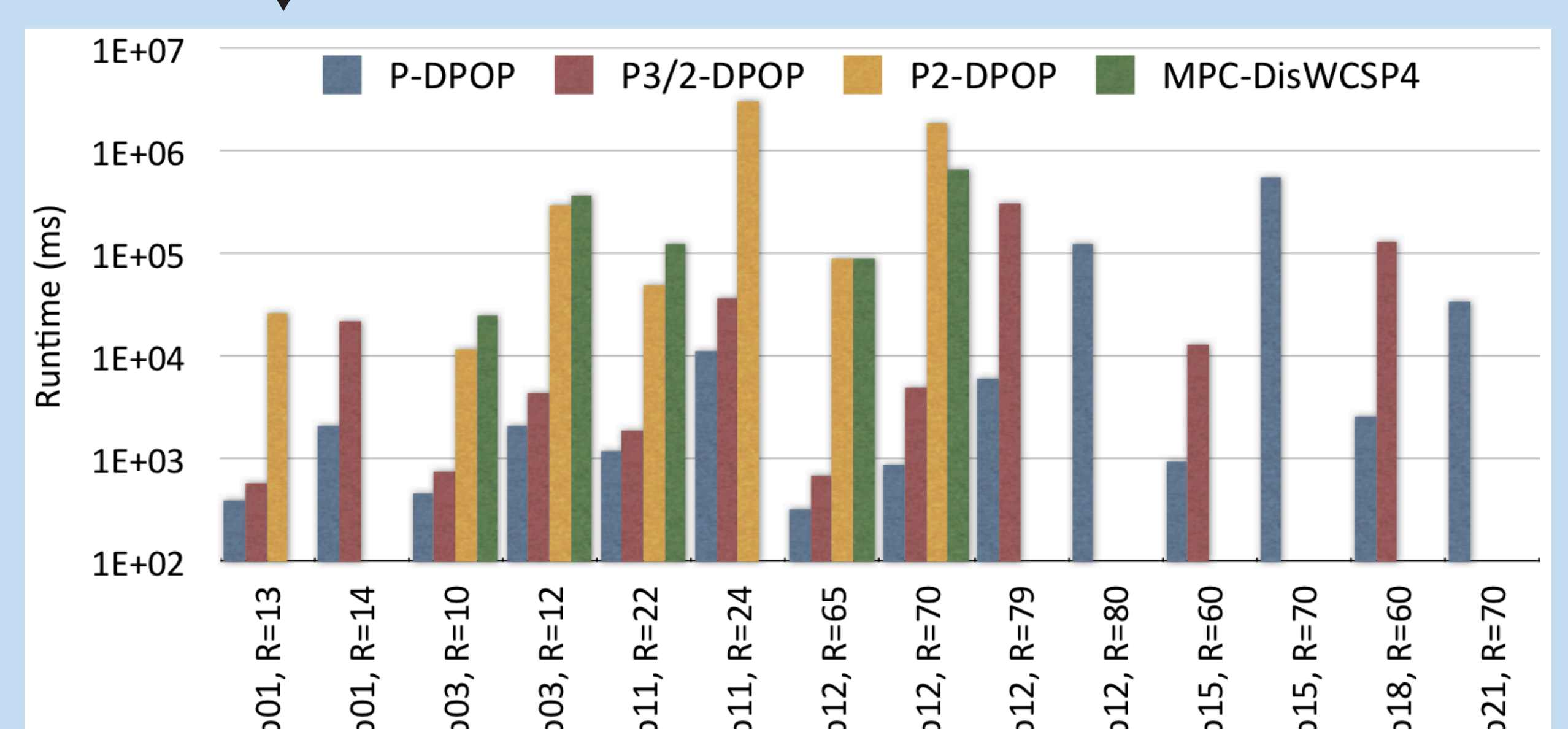
Privacy Definitions:

- **Agent privacy:** hiding unrelated agents
- **Topology privacy:** hiding unrelated topological constructs of the constraint graph
- **Constraint privacy:** hiding unrelated costs
- **Decision privacy:** hiding the values chosen for other agents' variables

Privacy Leaks:

- P*-DPOP has minor leaks of topology privacy (such as bounds on variable degrees)
- P²-DPOP uses weak encryption of constraint costs
- P-DPOP leaks final values of neighboring variables
- MPC-DisWCSP4 is subject to collusions by a majority of agents

Performance Evaluation



VRP Benchmarks:

- Based on standard Multiple-Depot VRP benchmarks by Cordeau
- Adapted to allow for split deliveries, and to vary the radius of operations