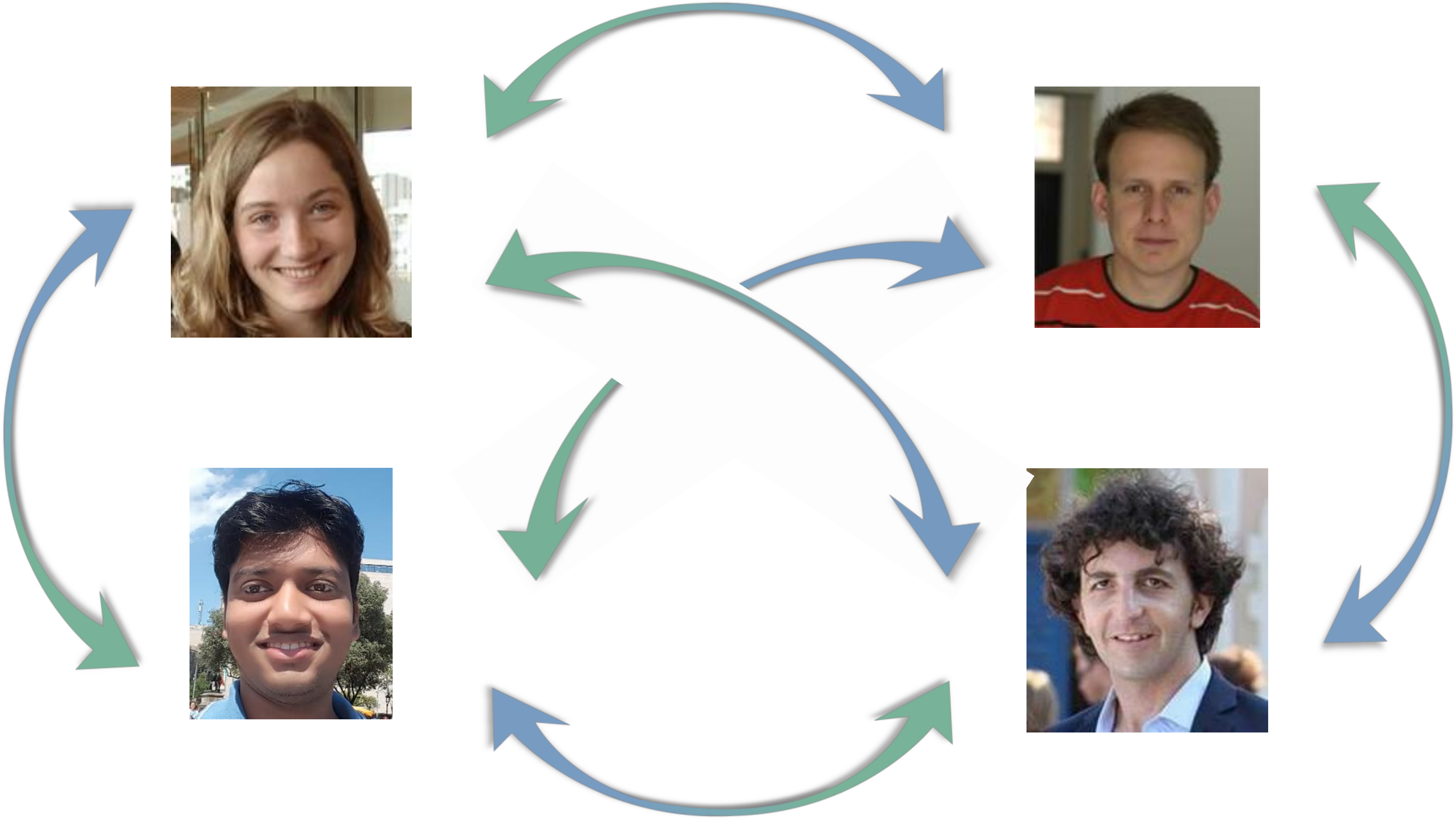
Must the Communication Graph of MPC Protocols be an Expander?

Elette Boyle (IDC)
Ran Cohen (MIT & Northeastern)
Deepesh Data (UCLA)
Pavel Hubacek (Charles University)

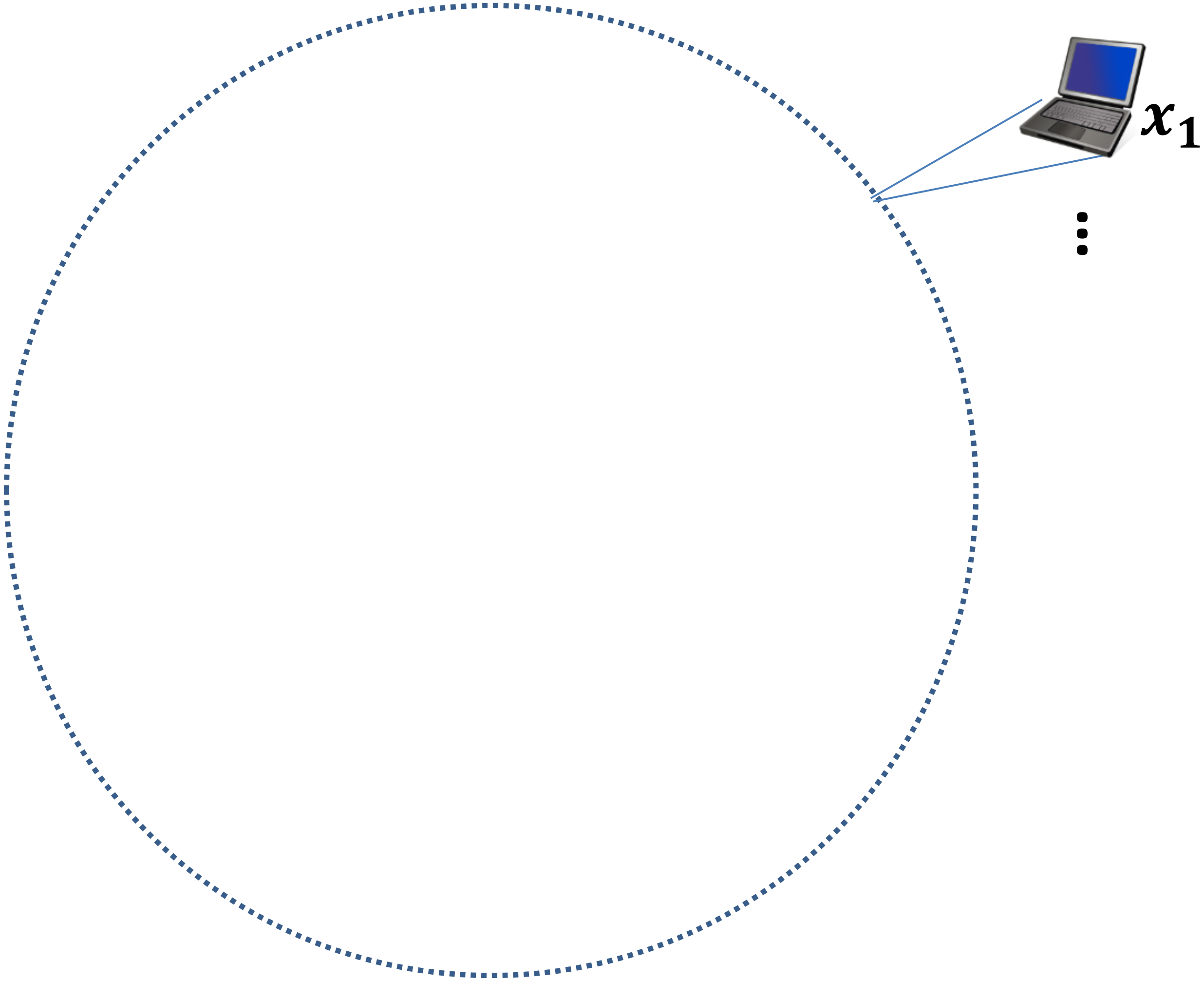
Secure Multiparty Computation



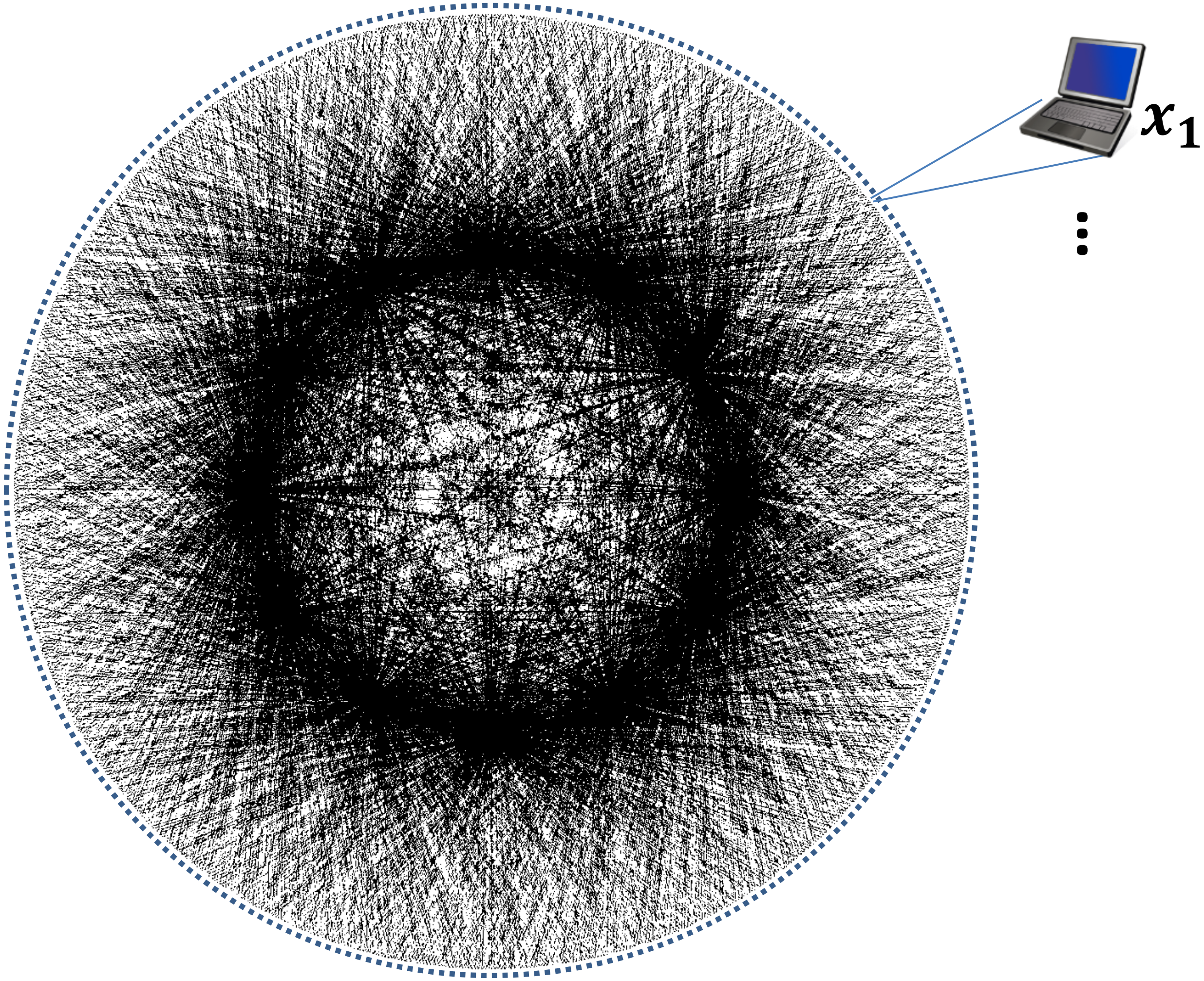
Secure Multiparty Computation

Every party talks to every party

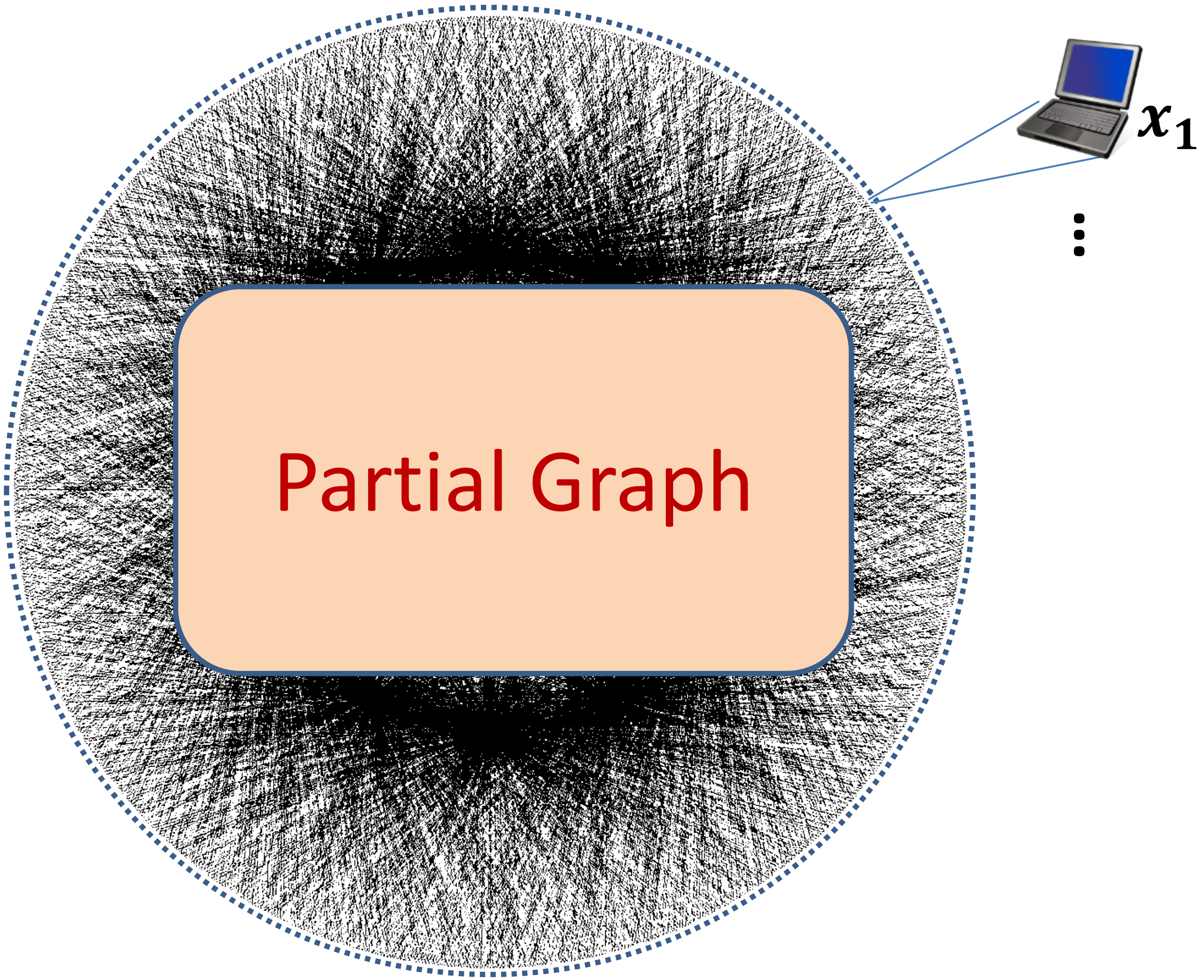
Large-Scale MPC



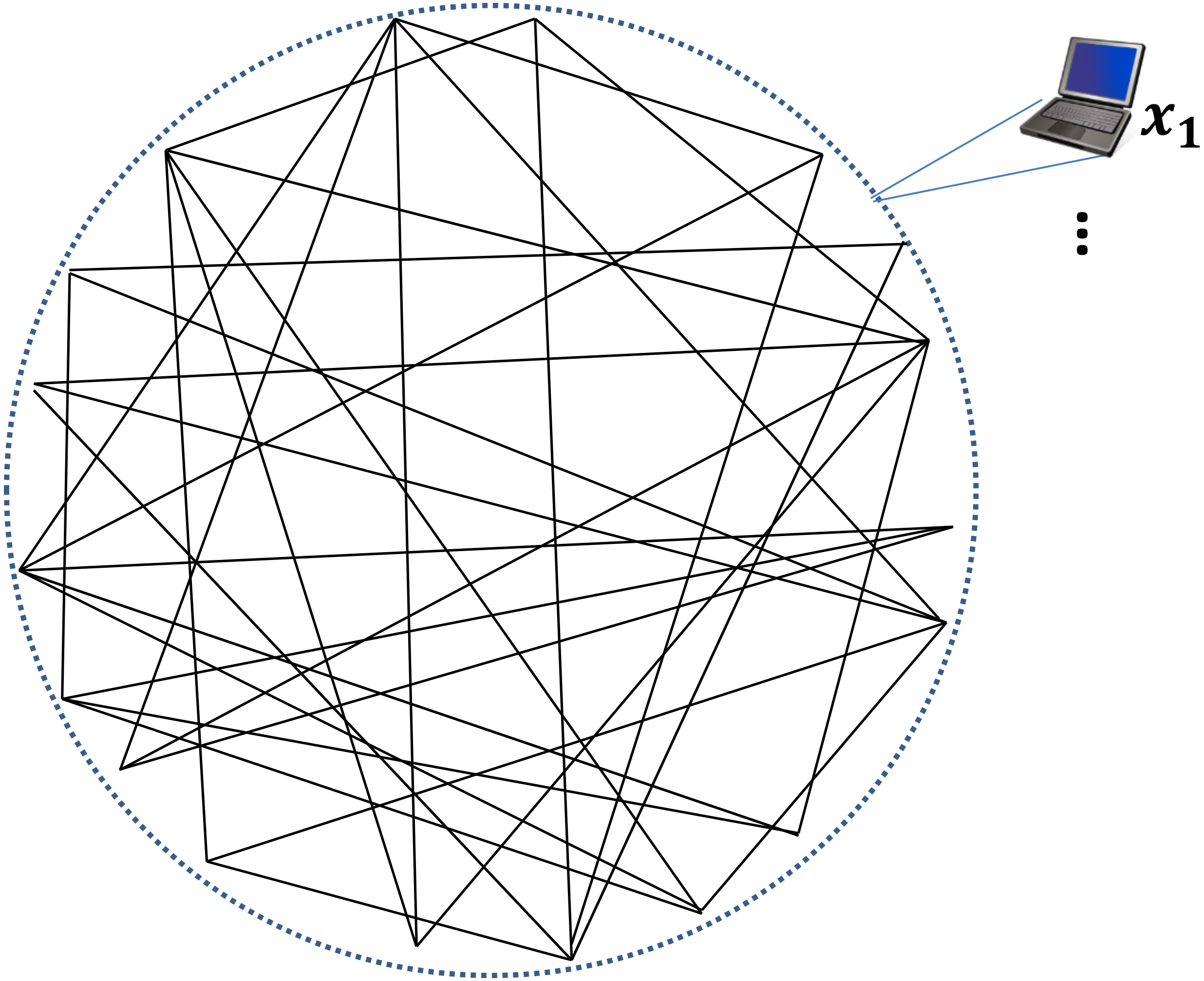
Large-Scale MPC



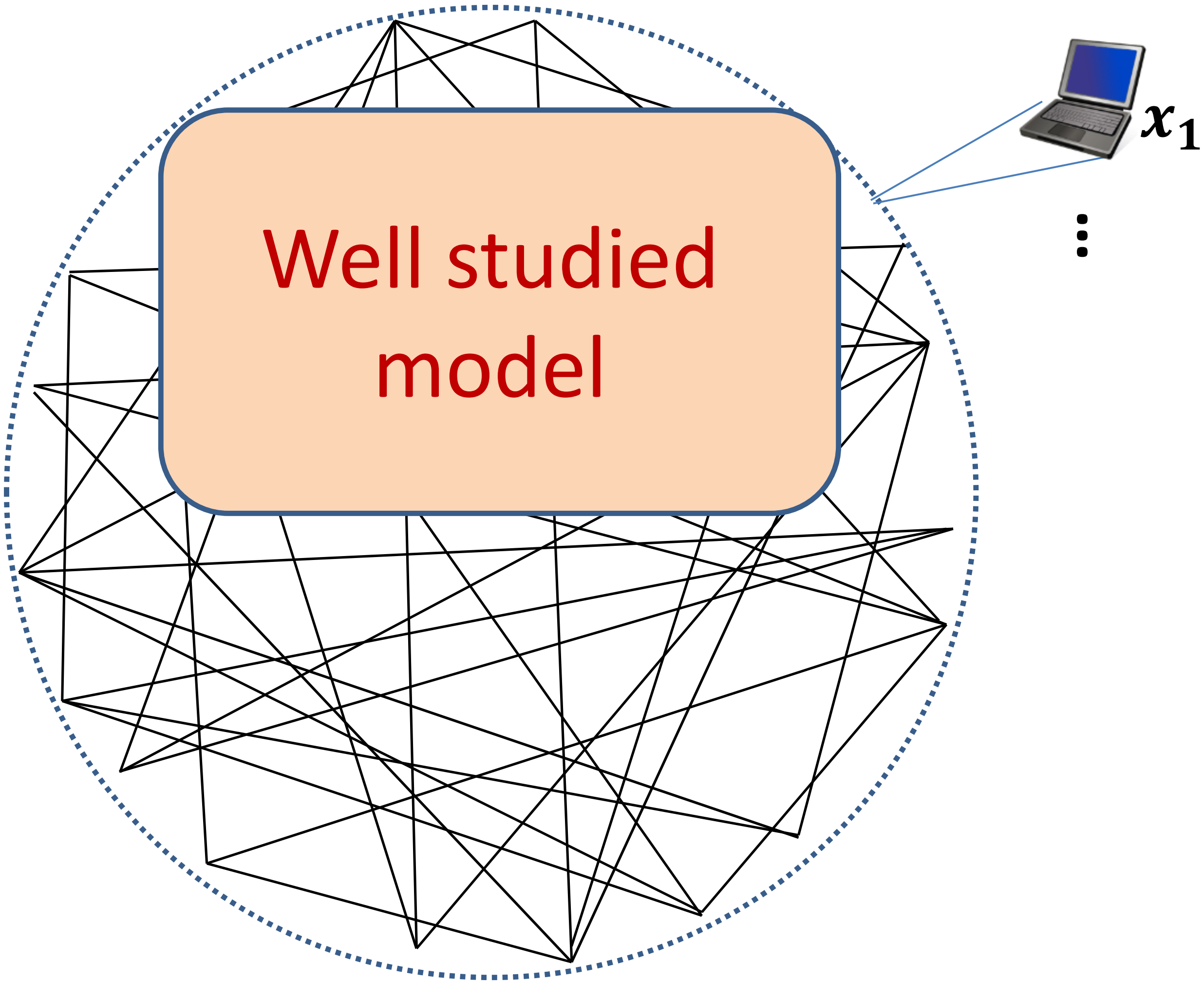
Large-Scale MPC



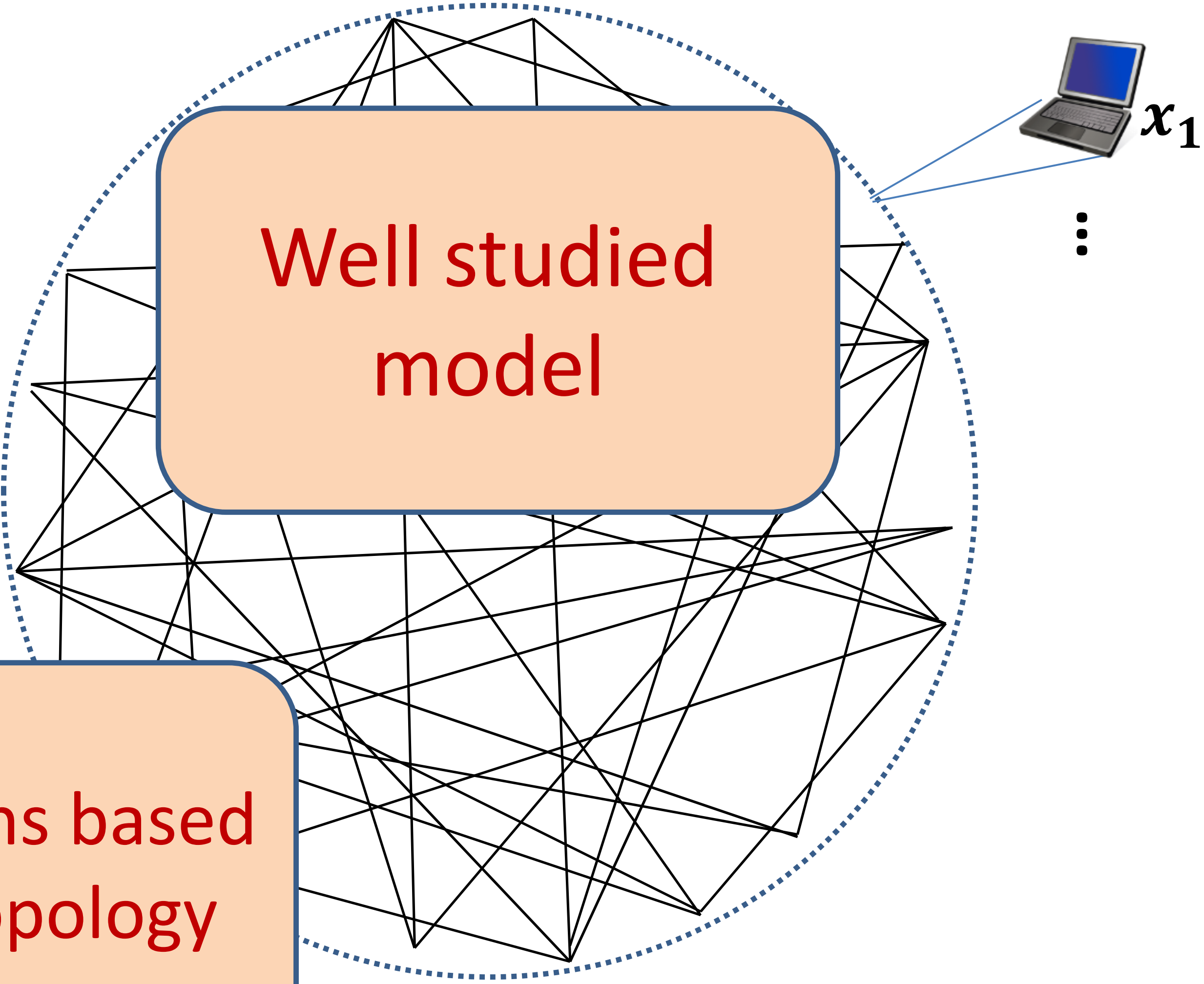
1) Fixed Partial Graph



1) Fixed Partial Graph



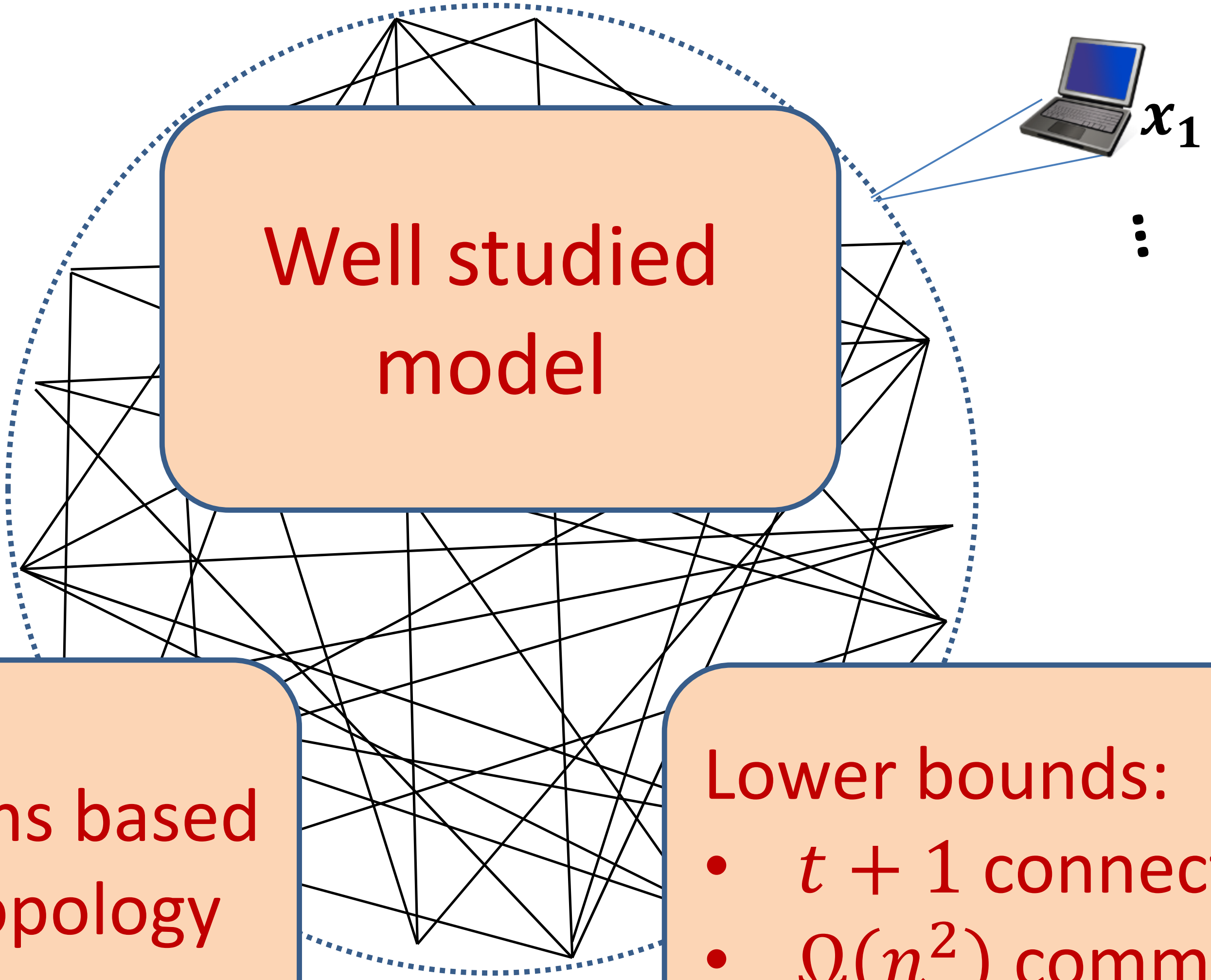
1) Fixed Partial Graph



Well studied model

Corruptions based on the topology

1) Fixed Partial Graph



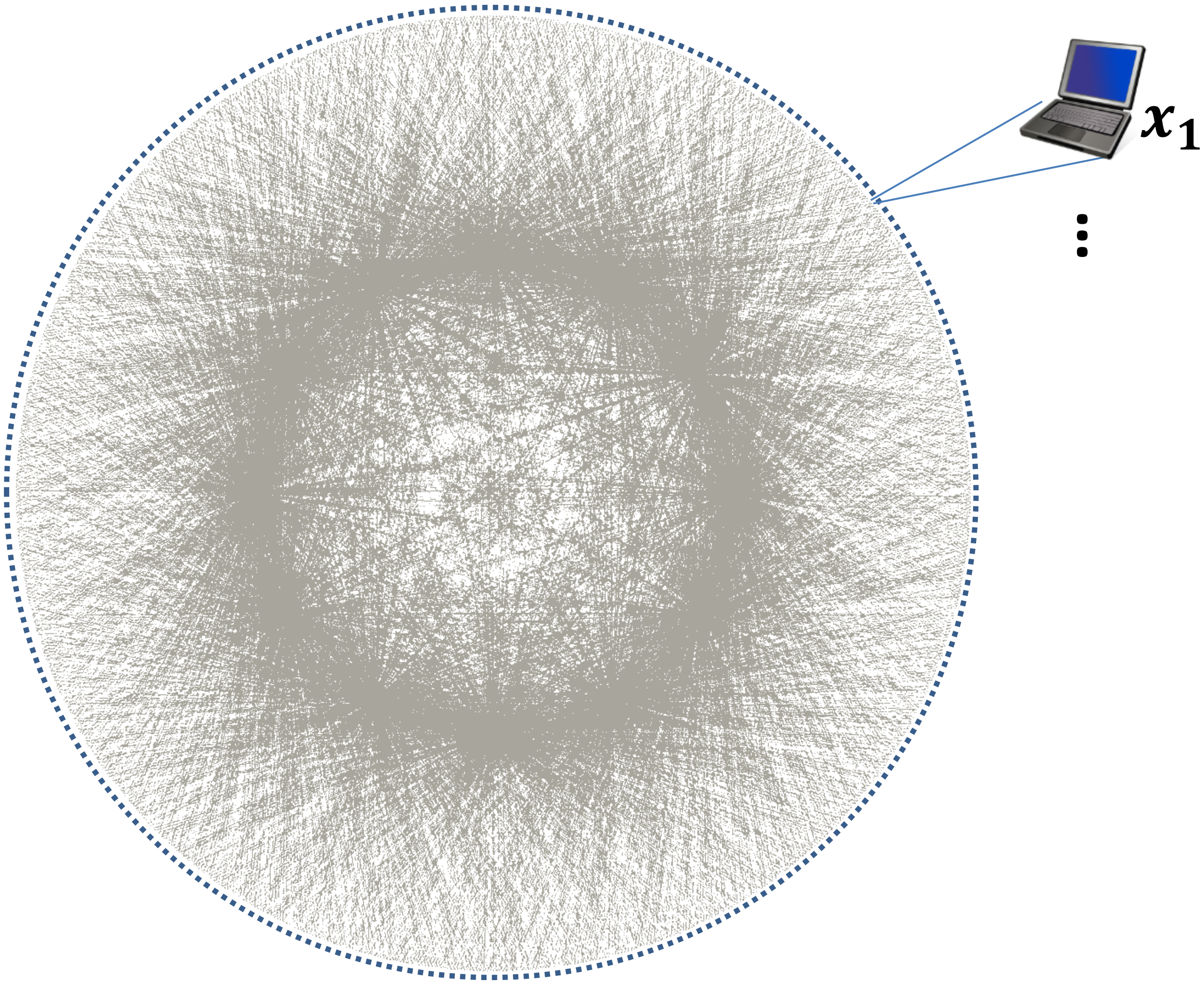
Well studied model

Corruptions based on the topology

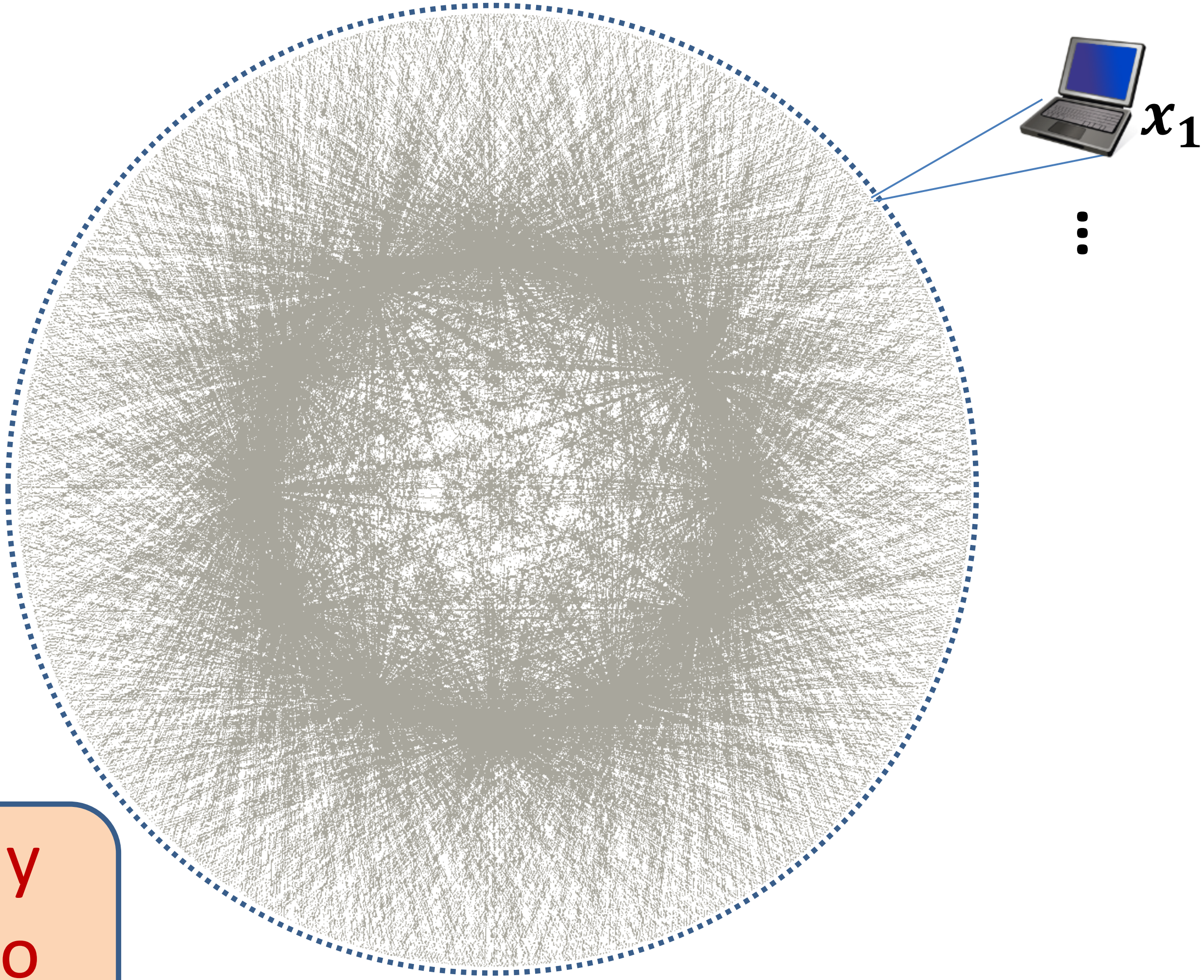
Lower bounds:

- $t+1$ connectivity
- $\Omega(n^2)$ comm.

2) Dynamic Partial Graph

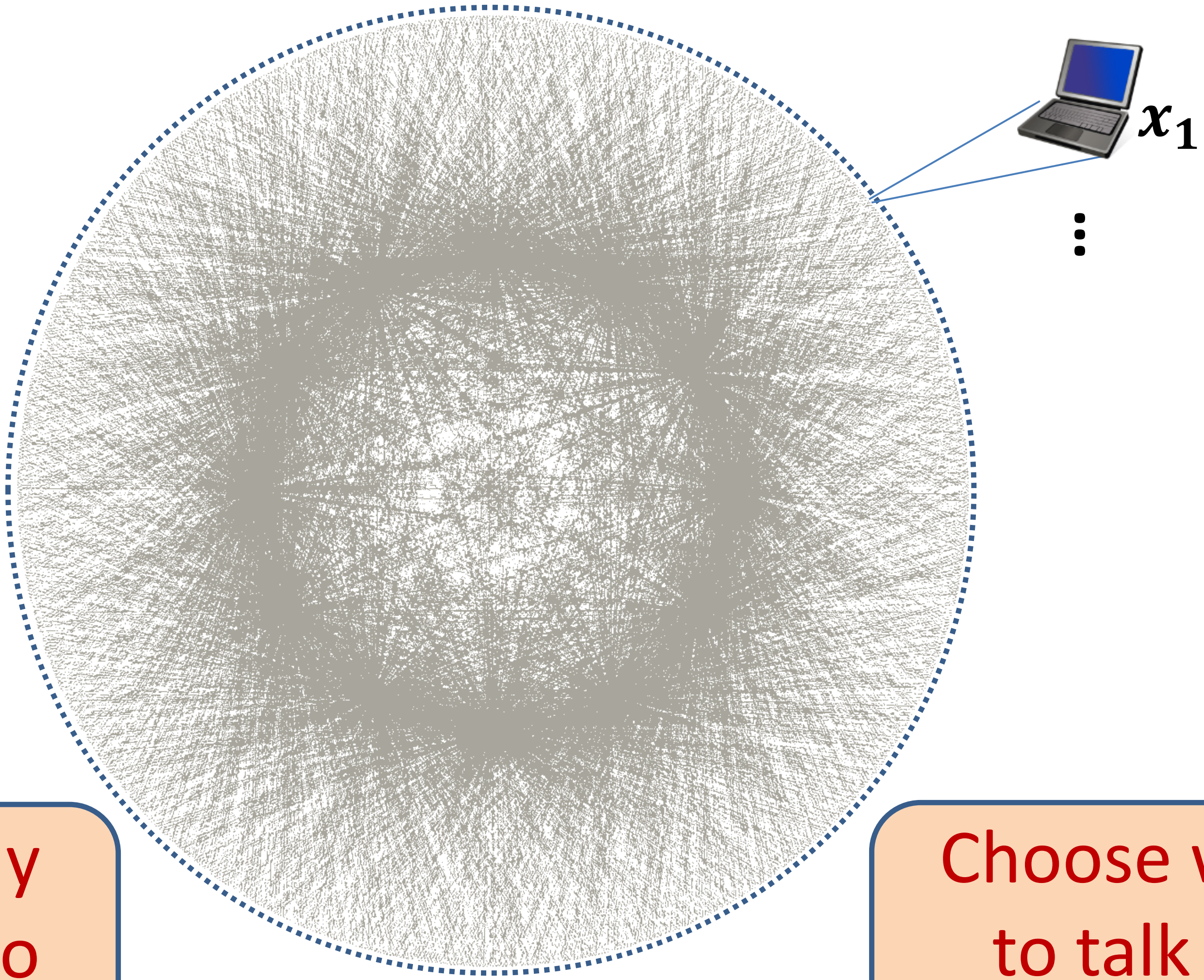


2) Dynamic Partial Graph



Everybody **can** talk to everybody

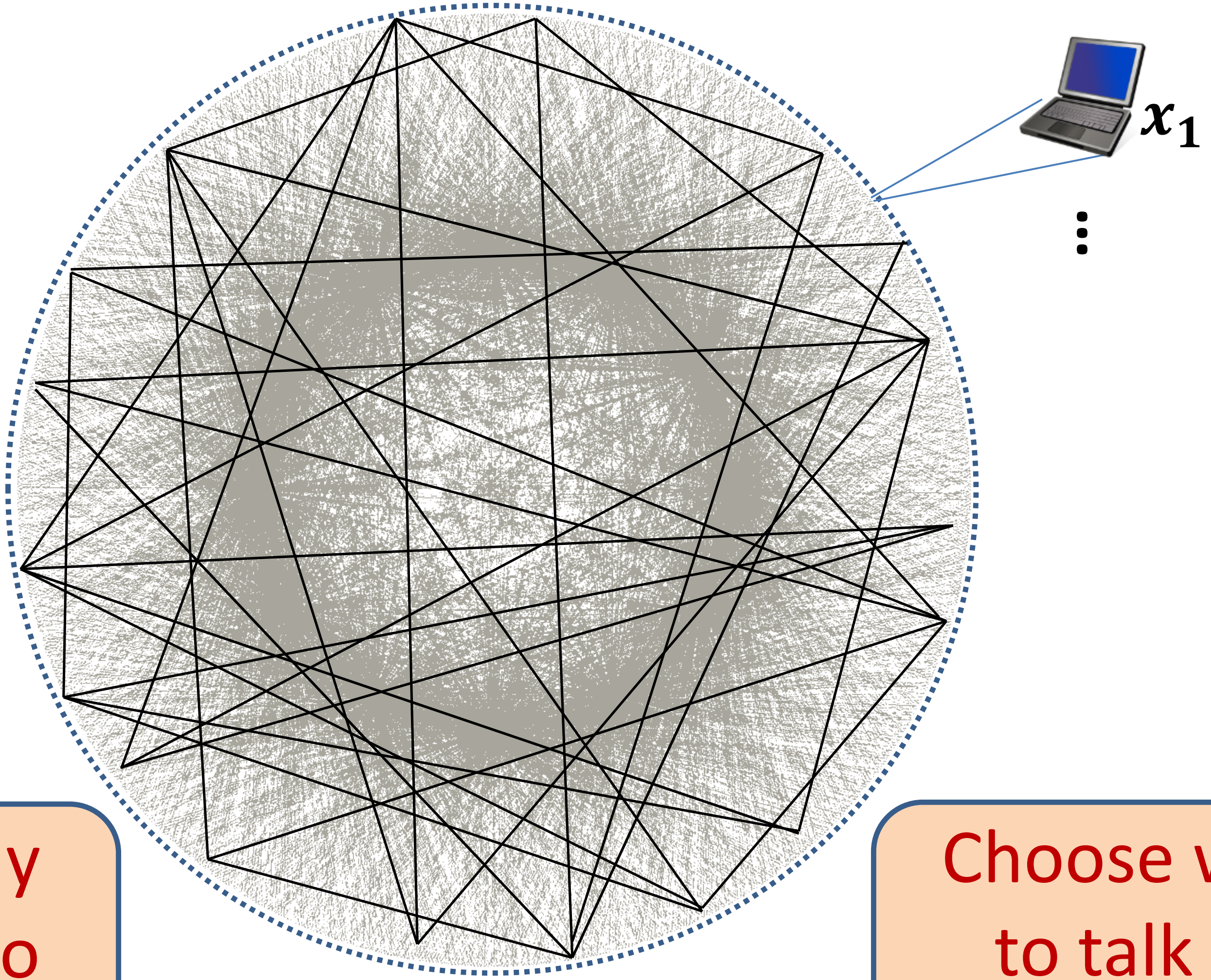
2) Dynamic Partial Graph



Everybody **can** talk to everybody

Choose who to talk to dynamically

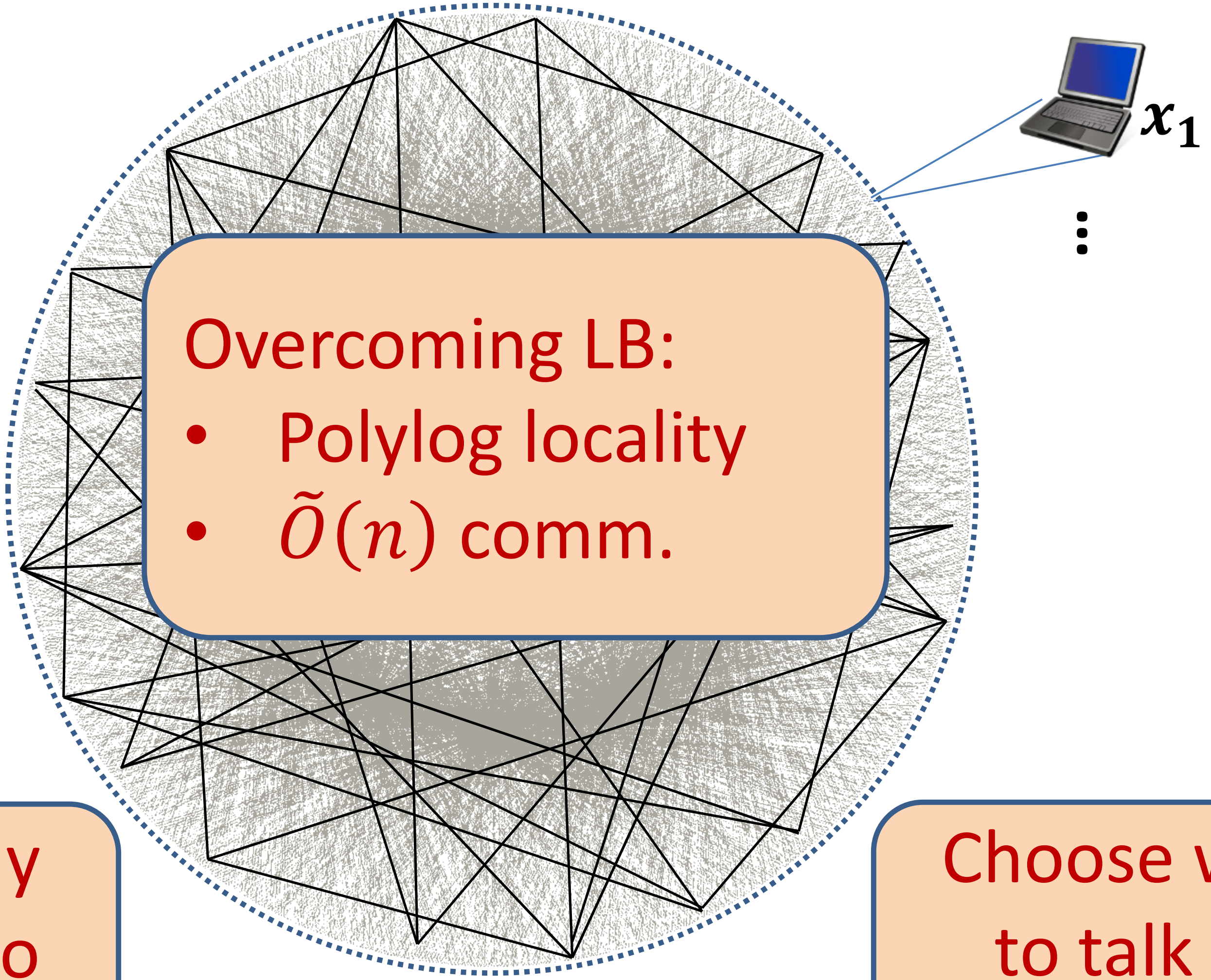
2) Dynamic Partial Graph



Everybody **can** talk to everybody

Choose who to talk to dynamically

2) Dynamic Partial Graph



Overcoming LB:

- Polylog locality
- $\tilde{O}(n)$ comm.

Everybody **can** talk to everybody

Choose who to talk to dynamically

Main Question

What graph properties are necessary to support secure protocols?

This Work

- Foundational study of dynamic graph model

This Work

- Foundational study of dynamic graph model
- Framework for analyzing various graph properties

This Work

- Foundational study of dynamic graph model
- Framework for analyzing various graph properties
- E.g., all existing protocols yield **expander** graphs

Sparse graphs with strong connectivity properties

This Work

- Foundational study of dynamic graph model
- Framework for analyzing various graph properties
- E.g., all existing protocols yield **expander** graphs
- Is this inherent?

Sparse graphs with strong connectivity properties

This Work

- Foundational study of dynamic graph model
- Framework for analyzing various graph properties
- E.g., all existing protocols yield **expander** graphs
- Is this inherent?
- It depends…

Sparse graphs with strong connectivity properties

This Work

- Foundational study of dynamic graph model
- Framework for analyzing various graph properties
- E.g., all existing protocols yield **expander** graphs
- Is this inherent?
- It depends…
  - – In many settings: **NO**
  - – In certain settings: **YES**

Sparse graphs with strong connectivity properties

Thank You