KU LEUVEN

Mariana Gama
KU Leuven

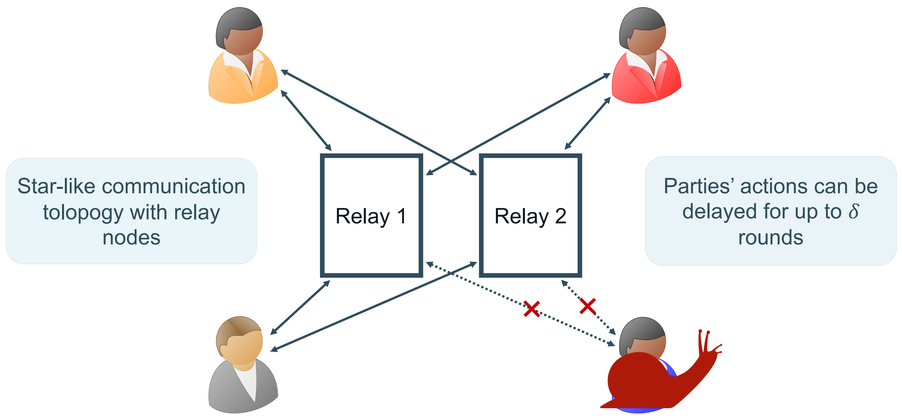
Emad Heydari Beni
KU Leuven
Nokia Bell Labs

Emmanuela Orsini
Uni. Bocconi

Nigel Smart
KU Leuven
Zama

Oliver Zajonc
KU Leuven

MPC with Delayed Parties Over Star-Like Networks

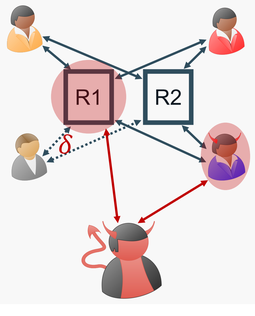


The protocol

- Based on Shamir Secret Sharing
- Multiplication with **1-round Damgård-Nielsen** protocol (using broadcast messages)
- **Active security** through circuit compilation as in Genkin et al. [GIP+14] (must be passively secure up to **additive attacks**)
- **Fast parties don't need to wait for delayed parties** (in the strong honest majority case)

The adversary

- Can corrupt up to $t < n/2$ parties (static corruption)
- Can corrupt all but one relay
- Can delay an arbitrary number of parties for up to δ rounds



Relay Interface

p2p messages

From party i to party j.

Commands:

Send: stores encrypted message to party j, round $k_{i,j}$
Request: retrieves message from i to j, round $k_{i,j}$
Erase: erases message from i to j, round $k_{i,j}$

Relay maintains:

- Pairwise message counter $k_{i,j}$
- Pairwise deleting counter $d_{i,j}$

Broadcast messages

From party i to all other parties.

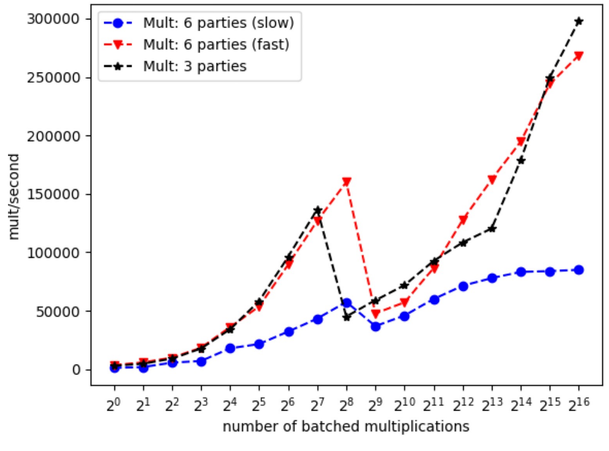
Commands:

SendToAll: stores plaintext message to all parties, round k^{all}
RequestFromAll: retrieves all messages for round k^{all}
EraseAll: erases all messages for round k^{all}

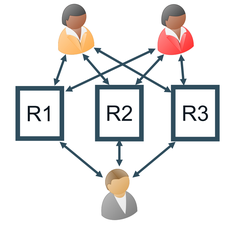
Relay maintains:

- Global message counter k^{all}
- Global deleting counter d^{all}

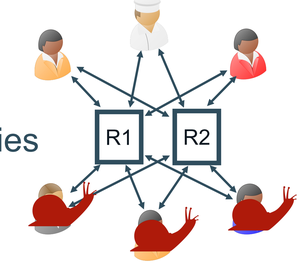
Cheap in a relay based network!



3 parties:
- At most 1 corruption



6 parties:
- At most 1 corruption
- 3 slow parties, 3 fast parties



Faster parties:
~270k multiplications/s