Brief Announcement: **Communication-Optimal Convex Agreement**

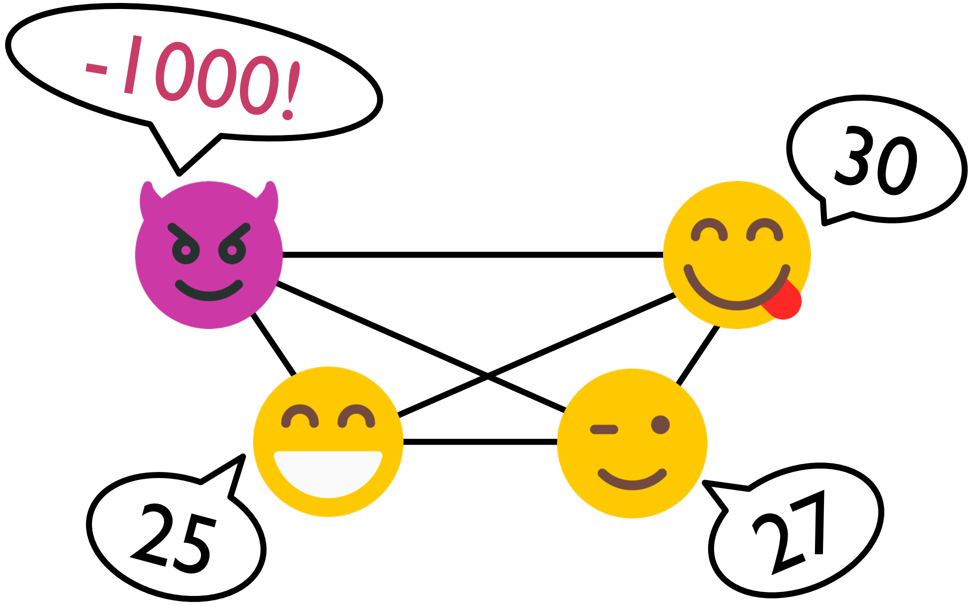
Diana Ghinea[★], Chen-Da Liu-Zhang[✤], Roger Wattenhofer[★]

[★] ETH Zürich

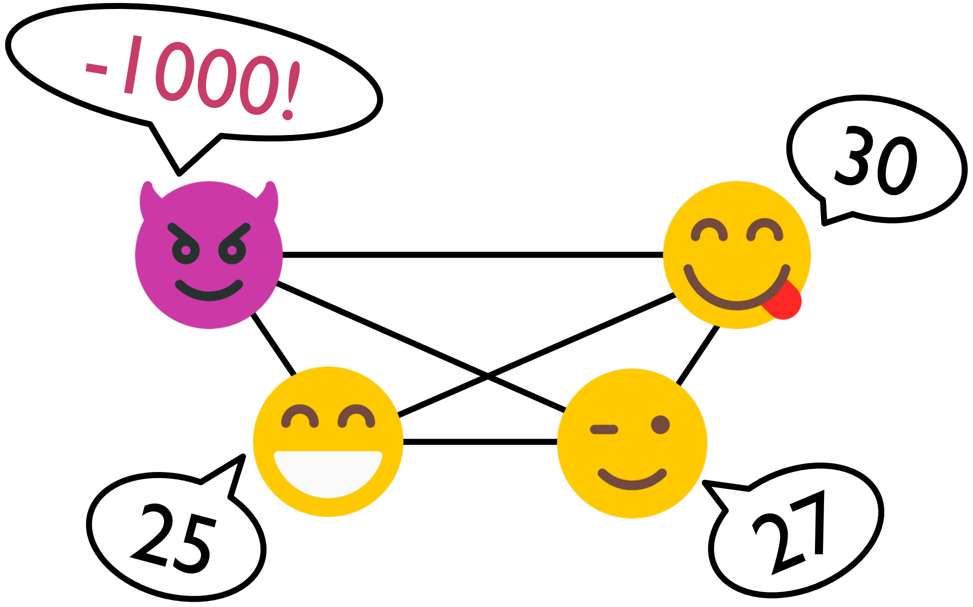
[✤] Lucerne University of Applied Sciences and Arts & Web3 Foundation

Byzantine Agreement

- Consider n parties; $t < n/3$ of them byzantine.
- The network is synchronous.
- Each party has an input.
- Honest parties need to **agree** on a value…

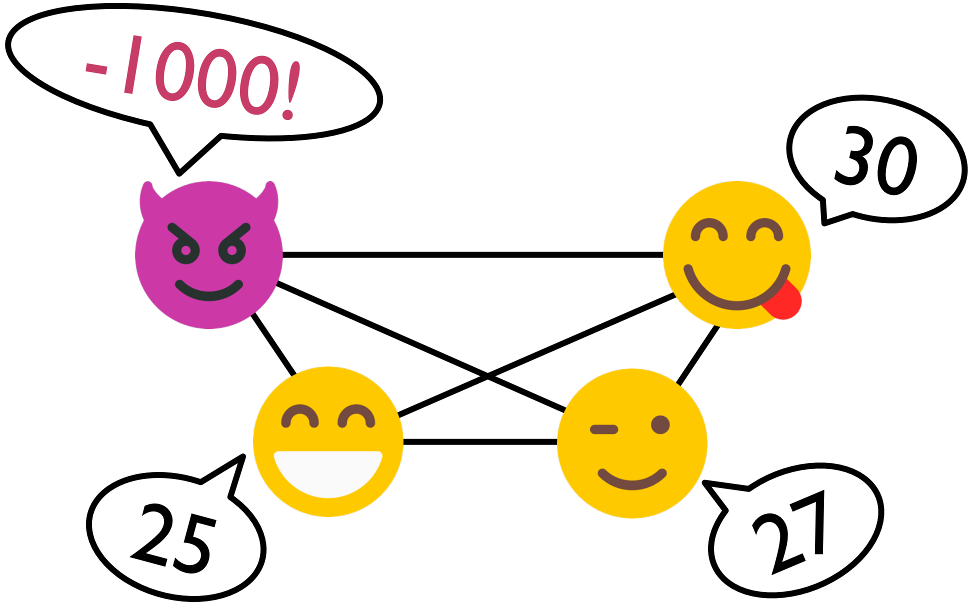


Byzantine Agreement



- Consider n parties; $t < n/3$ of them byzantine.
- The network is synchronous.
- Each party has an input.
- Honest parties need to **agree** on a value…
  - … satisfying the following **validity** condition:
    - **If all honest parties have input v, then the output agreed upon is v.**
    - **So, if honest parties have different inputs, they can agree on any value.**

Convex Agreement



- Consider n parties; $t < n/3$ of them byzantine.
- The network is synchronous.
- Each party has an input **(for today in $\mathbb{Z}$)**.
- Honest parties need to **agree** on a value…
  - … satisfying the following **validity** condition:
    - ~~**If all honest parties have input v, then the output agreed upon is v.**~~
    - ~~**So, if honest parties have different inputs, they can agree on any value.**~~
    - **The output agreed upon must be in the honest inputs' range.**

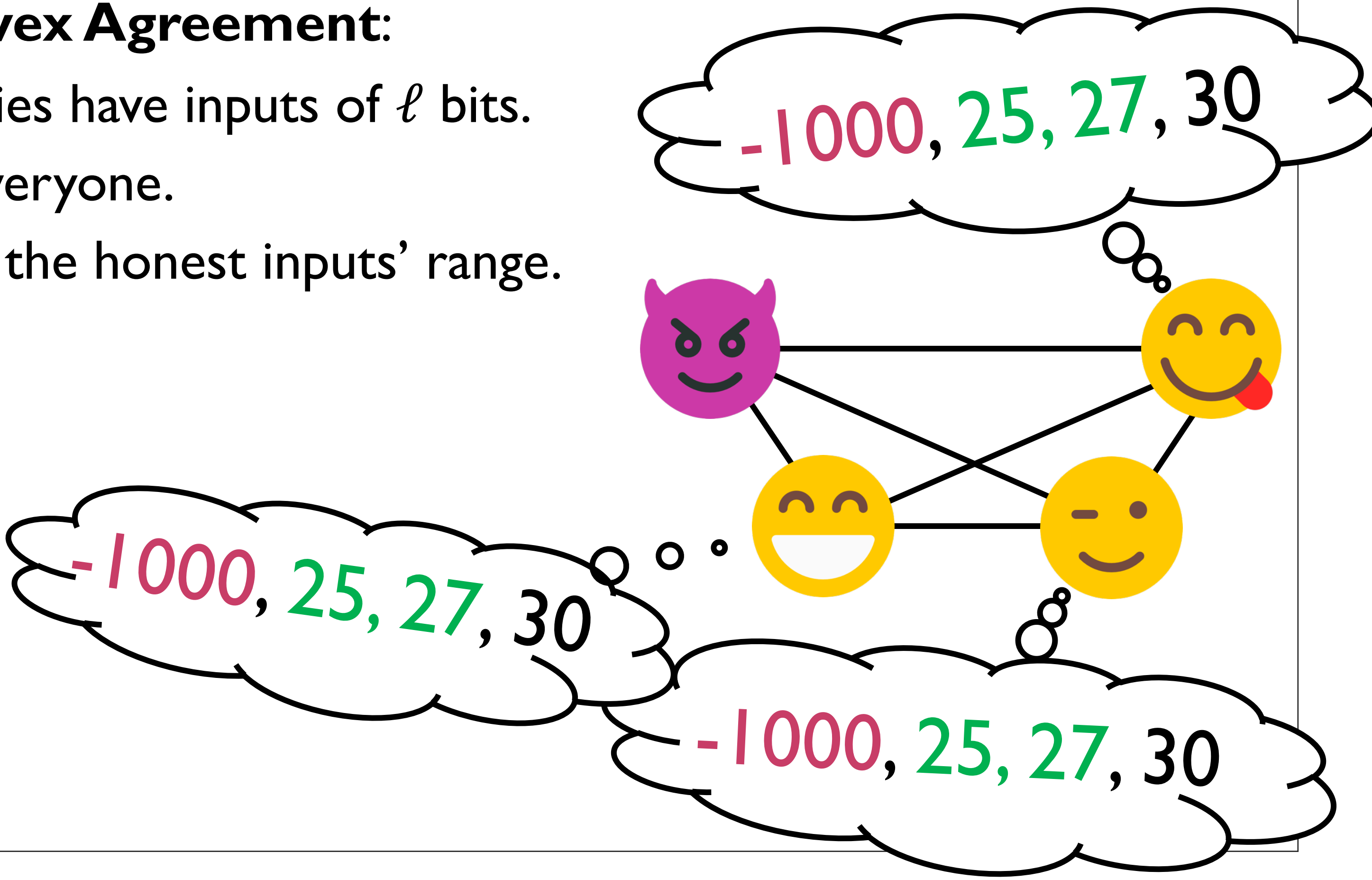
What is the optimal **communication complexity** for Convex Agreement?

= number of bits sent by the honest parties

assuming they have ℓ-bit inputs.

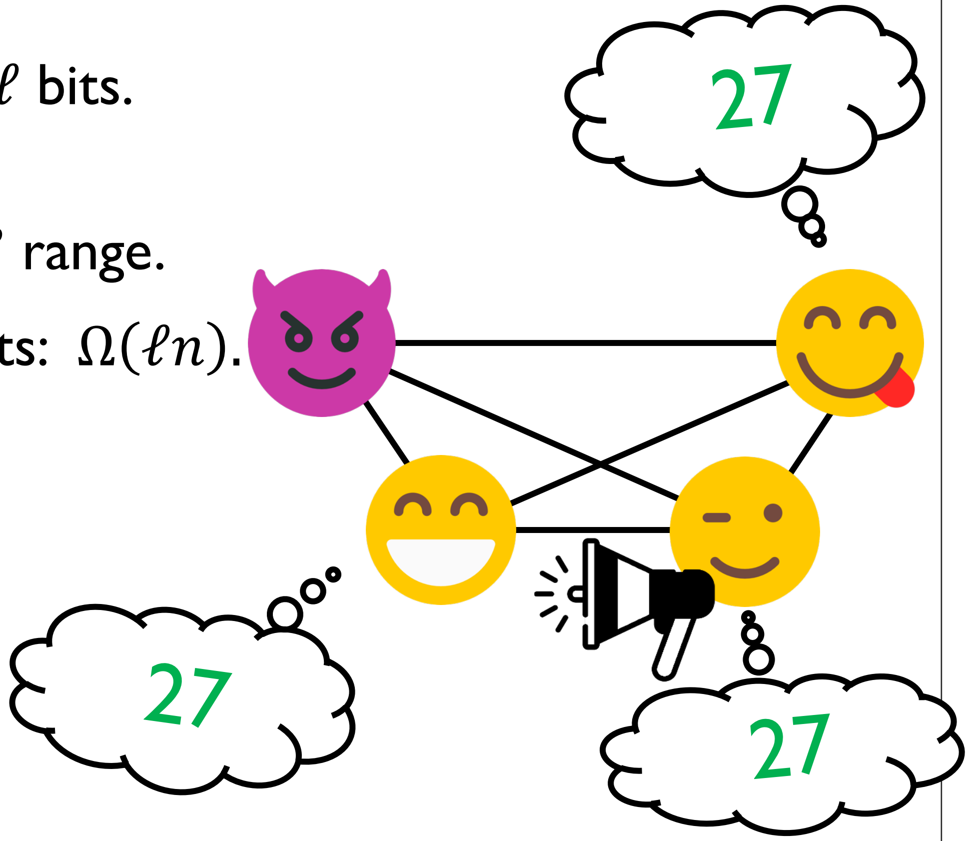
Communication Complexity

- State-of-the-art solutions for **Convex Agreement**:
  $O(\ell n^2)$ bits, assuming honest parties have inputs of ℓ bits.
  ~ every party sends its input to everyone.
  => parties gain information about the honest inputs' range.



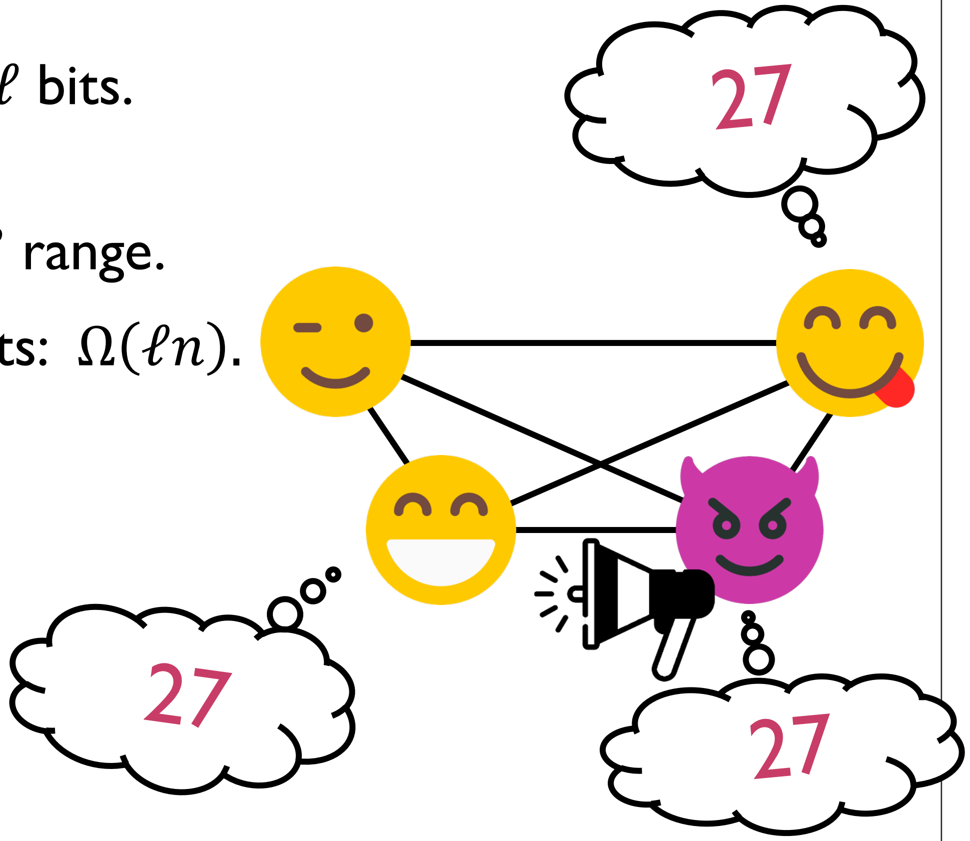
Communication Complexity

- State-of-the-art solutions for **Convex Agreement**:
  $O(\ell n^2)$ bits, assuming honest parties have inputs of ℓ bits.
  ~ every party sends its input to everyone.
  => parties gain information about the honest inputs' range.
- A **lower bound**, if honest parties have inputs of ℓ bits: $\Omega(\ell n)$.
  ~ one honest party sends its input to everyone.



Communication Complexity

- State-of-the-art solutions for **Convex Agreement**:
  $O(\ell n^2)$ bits, assuming honest parties have inputs of ℓ bits.
  ~ every party sends its input to everyone.
  => parties gain information about the honest inputs' range.
- A **lower bound**, if honest parties have inputs of ℓ bits: $\Omega(\ell n)$.
  ~ one honest party sends its input to everyone.
  => less information about the honest inputs' range.



Communication Complexity

- State-of-the-art solutions for **Convex Agreement**:
  $O(\ell n^2)$ bits, assuming honest parties have inputs of ℓ bits.
  ~ every party sends its input to everyone.
  => parties gain information about the honest inputs' range.
- A **lower bound**, if honest parties have inputs of ℓ bits: $\Omega(\ell n)$.
  ~ one honest party sends its input to everyone.
  => less information about the honest inputs' range.
- For **Byzantine Agreement**, $O(\ell n)$ bits are sufficient (for large enough ℓ)!
  However, existing solutions lose information about the honest inputs' range.

Our Result

- Convex Agreement can be achieved with asymptotically optimal communication complexity $O(\ell n)$ for ℓ-bit inputs in $\mathbb{Z}$! (for $\ell > n^2 \log n \cdot$ security parameter size)
- Our solution is a byzantine variant of the ***longest common prefix*** problem.
- Take a look at out paper!

eprint.iacr.org/2024/251