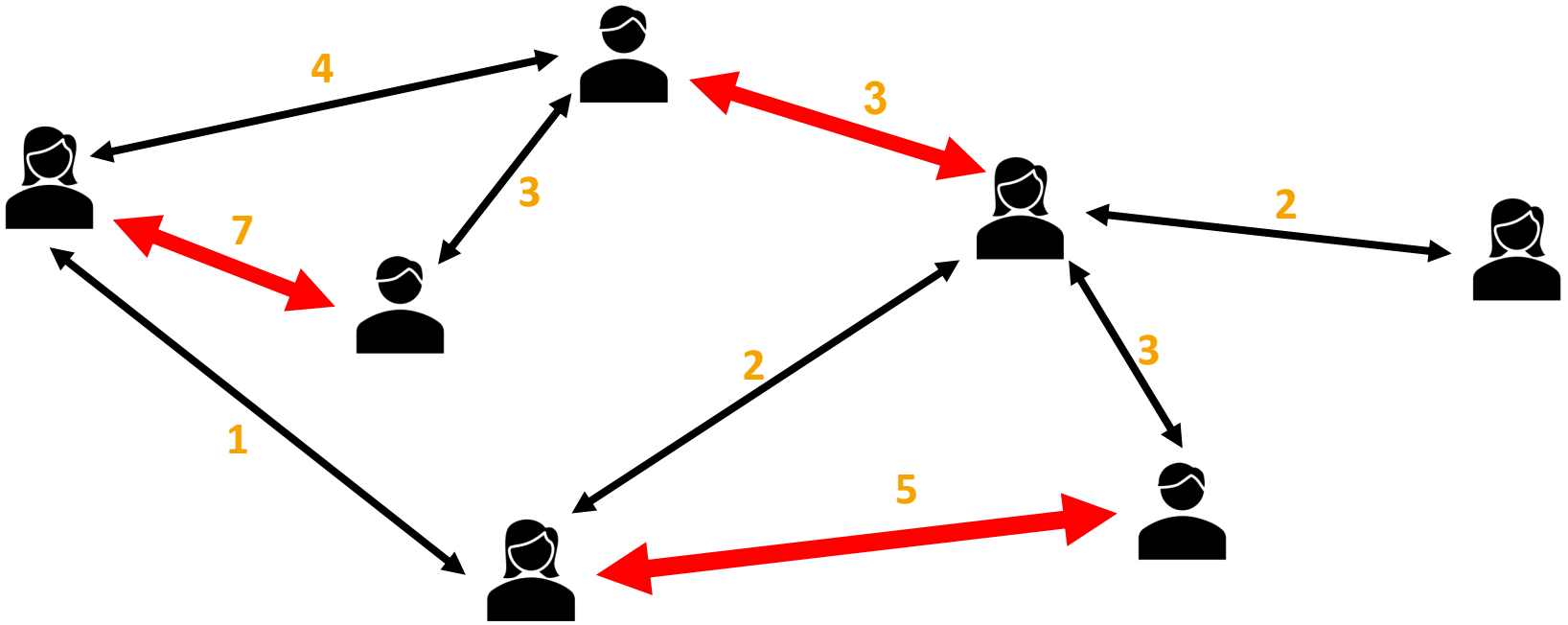
Secure Maximum Weight Matching Approximation on General Graphs

Andreas Brüggemann, Malte Breuer, Andreas Klinger, Thomas Schneider, Ulrike Meyer

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

RWTH AACHEN UNIVERSITY



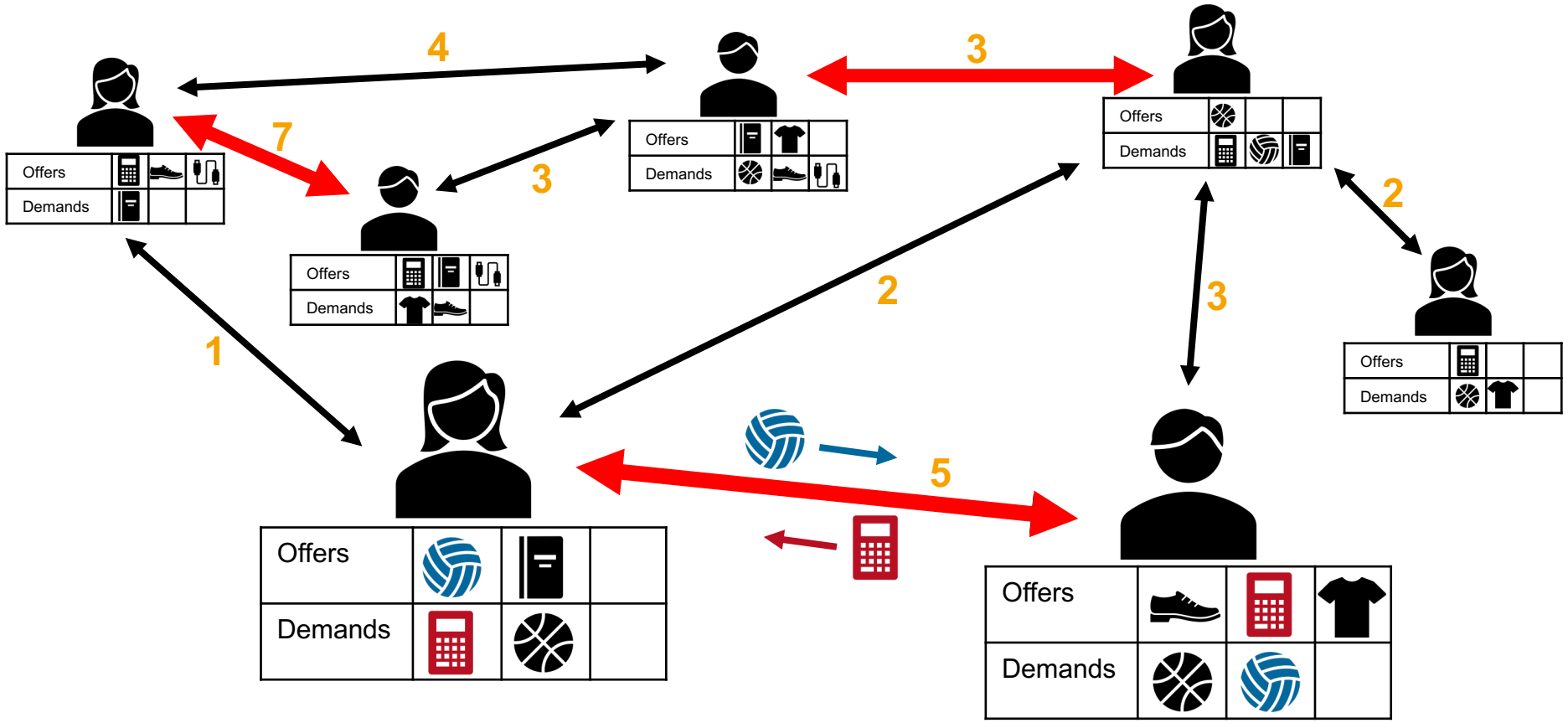
In This Talk

ENCRYPTO
CRYPTOGRAPHY AND PRIVACY ENGINEERING

- Maximum weight matching and its applications
- Privacy? → Secure Multi-Party Computation
- Approximation
- Observations & Results

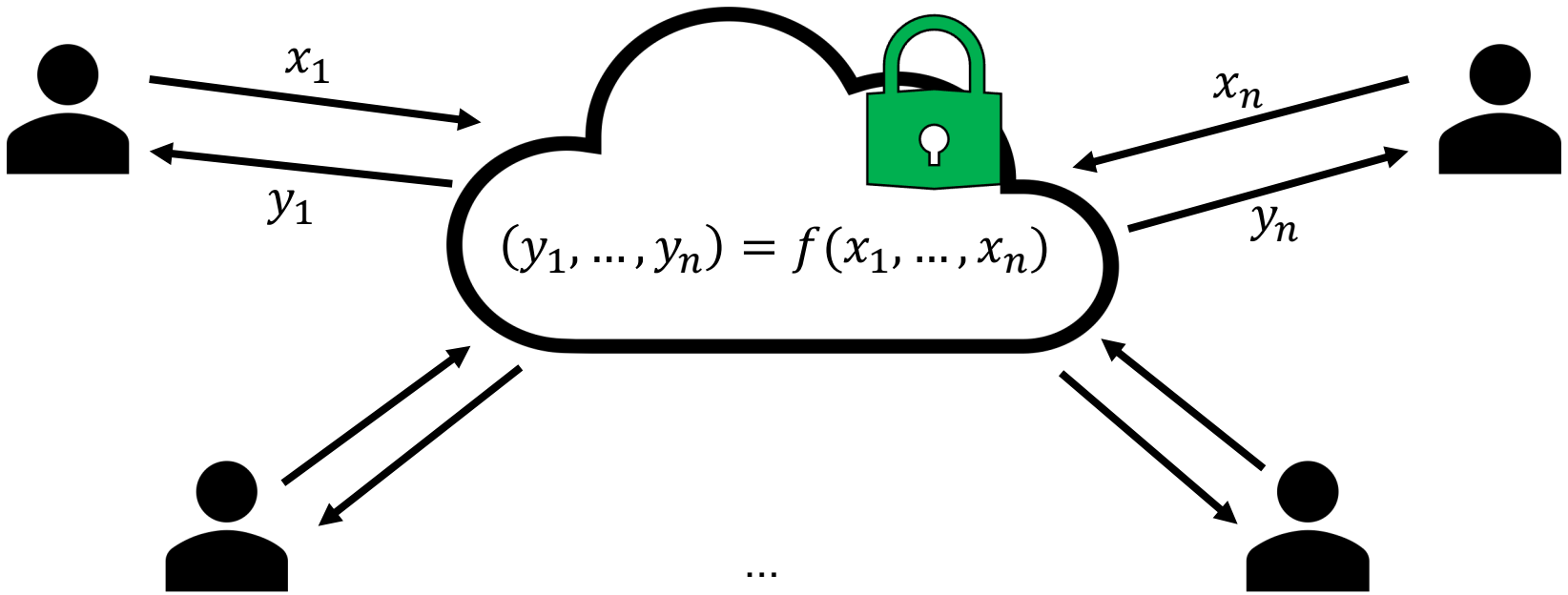
RWTH AACHEN UNIVERSITY
TECHNISCHE UNIVERSITÄT DARMSTADT

Maximum Weight Matching (for Bartering)



Privacy? → Secure Multi-Party Computation

- Bartering → Protect users' offers & demands
- Online dating → Protect users' sexual orientation, interests, …
- Kidney transplantation → Protect sensitive medical information



Related Work

- Prior research focused on MPC protocols for bipartite (i.e., between two groups) matchings, e.g., [BS15], [DES16]
- Only one protocol for general graphs (maximum matching) [BMW22]
  → $\mathcal{O}(N^5)$ communication, 127 h run time for $N = 60$ nodes in a LAN

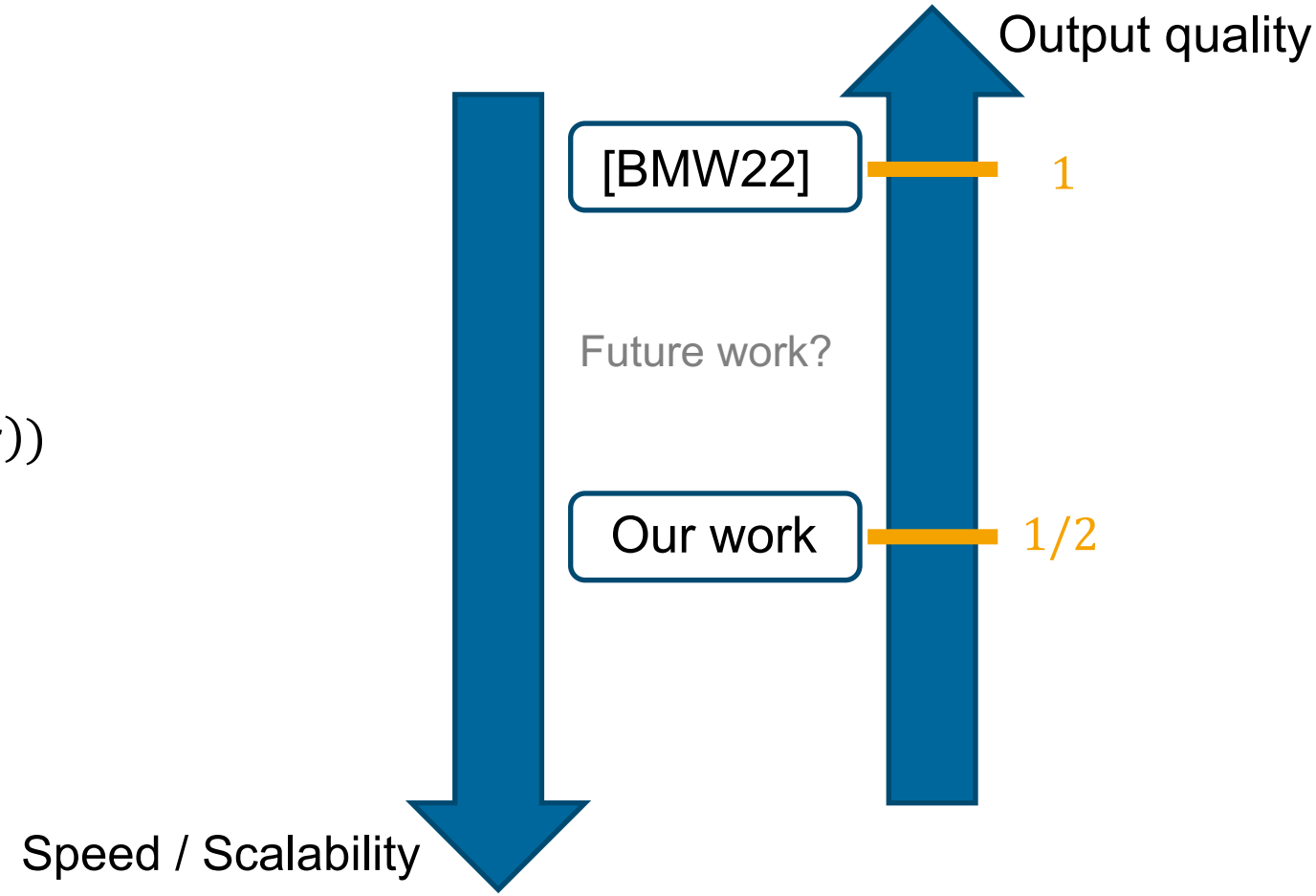
[BMW22] M. Breuer, U. Meyer, and S. Wetzel. **Privacy-Preserving Maximum Matching on General Graphs and its Application to Enable Privacy-Preserving Kidney Exchange.** In ACM CODASPY, 2022.

[BS15] M. Blanton and S. Saraph. **Oblivious Maximum Bipartite Matching Size Algorithm with Applications to Secure Fingerprint Identification.** In ESORICS, 2015.

[DES16] J. Doerner, D. Evans, and a. shelat. **Secure Stable Matching at Scale.** In ACM CCS, 2016.

Approximation: Compute a *Good* but not Optimal Solution

$$\text{gain}(\text{Alg}_{\text{exact}}(x)) \leq c \cdot \text{gain}(\text{Alg}_{\text{approx}}(x))$$



Approach: Greedy 1/2-Approximation

Greedy Algorithm [Avi83, Pre99]:

- Select heaviest edge, add to matching
- Delete this and all incident edges
- Repeat

Used Techniques

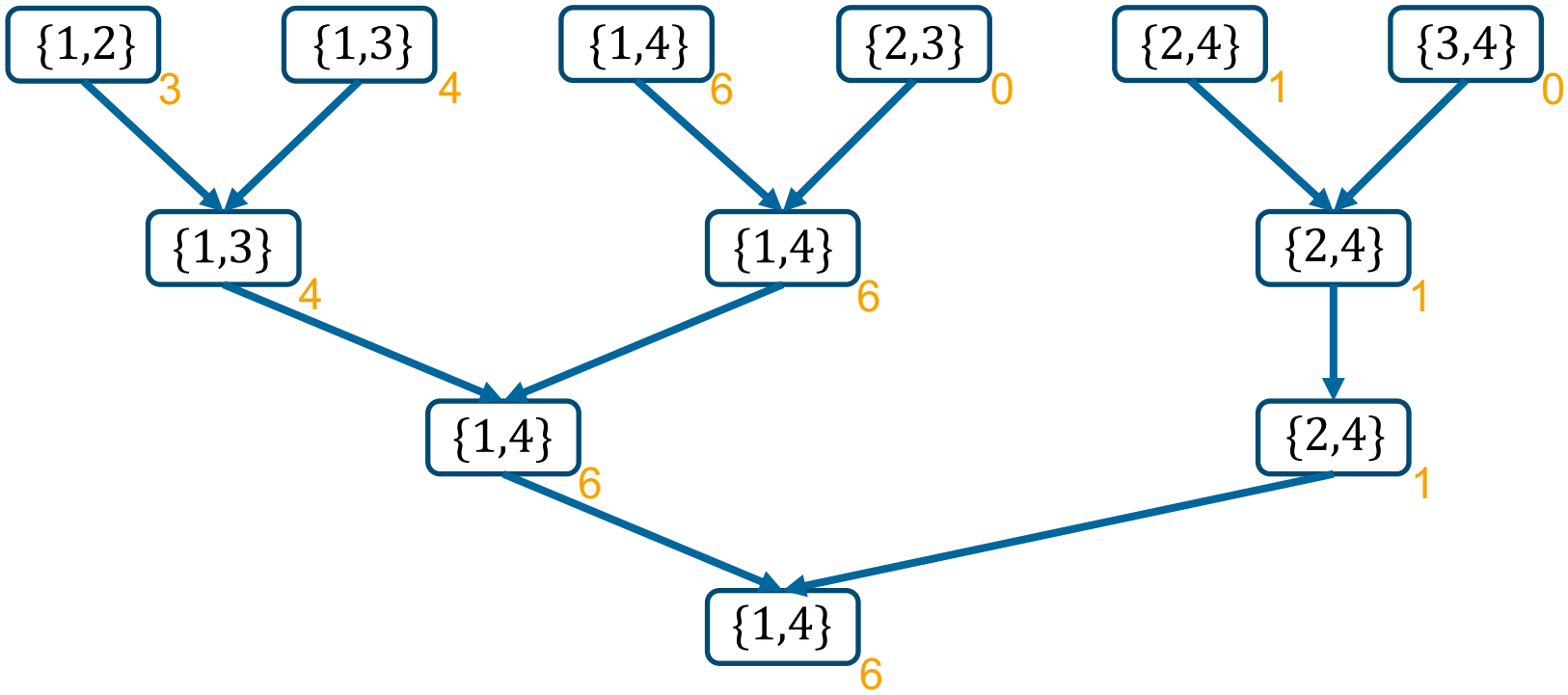
- Parallel reduction trees
- Randomization
- …

[Avi83] D. Avis. **A Survey of Heuristics for the Weighted Matching Problem.** In Networks (13), 1983.

[Pre99] R. Preis. **Linear Time 1/2-Approximation Algorithm for Maximum Weighted Matching in General Graphs.** In STACS, 1999.

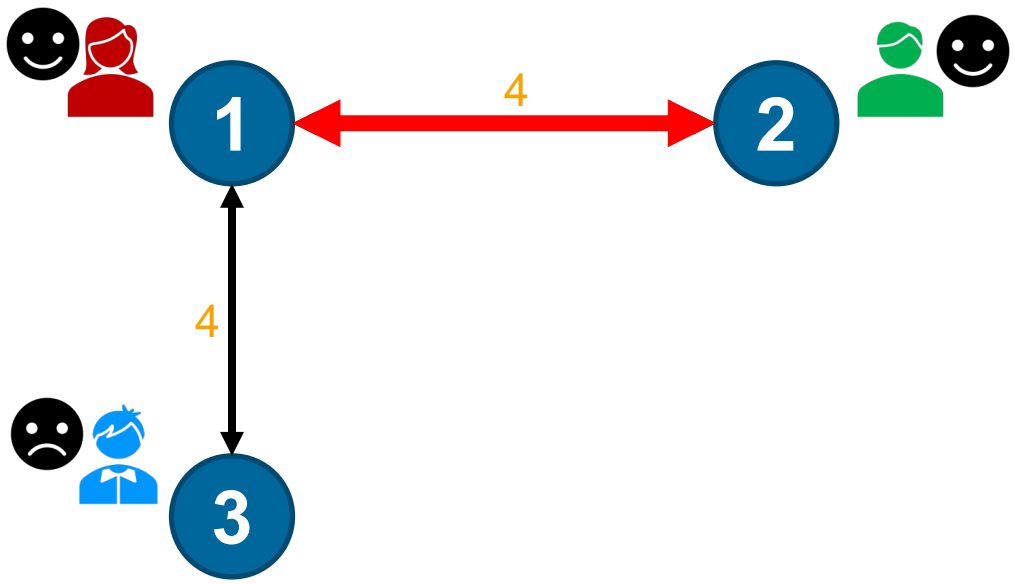
Parallel Reduction Trees

Searching heaviest edge: $\mathcal{O}(N^2)$ communication and rounds

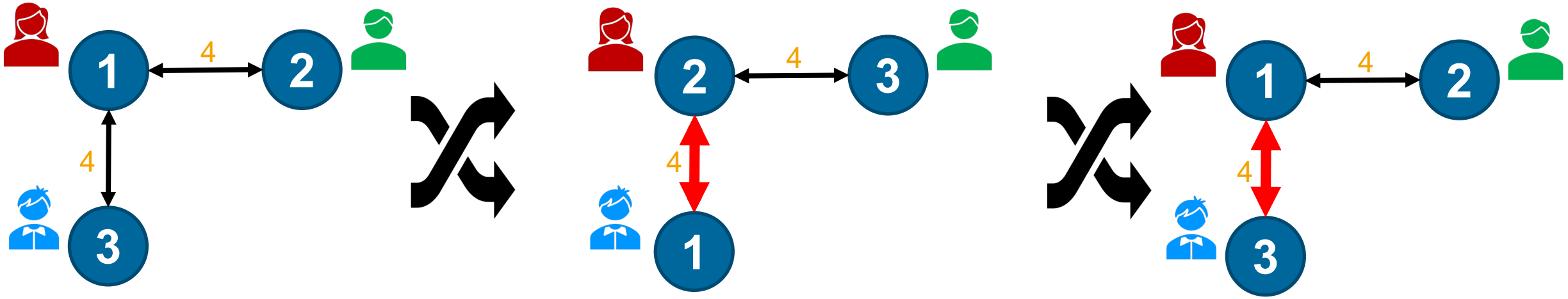


→$\mathcal{O}(N^2)$ communication, $\mathcal{O}(\log N)$ rounds

Node Label Bias



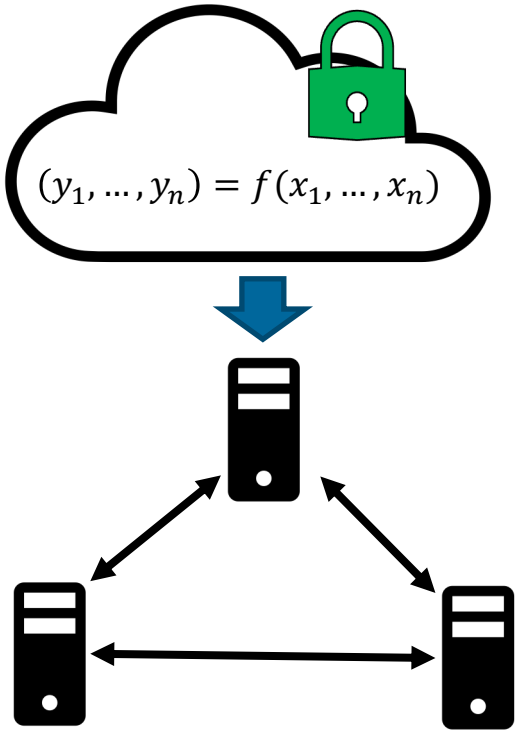
Randomization



Results I

- $\mathcal{O}(N^3)$ communication
- $\mathcal{O}(N \log N)$ rounds

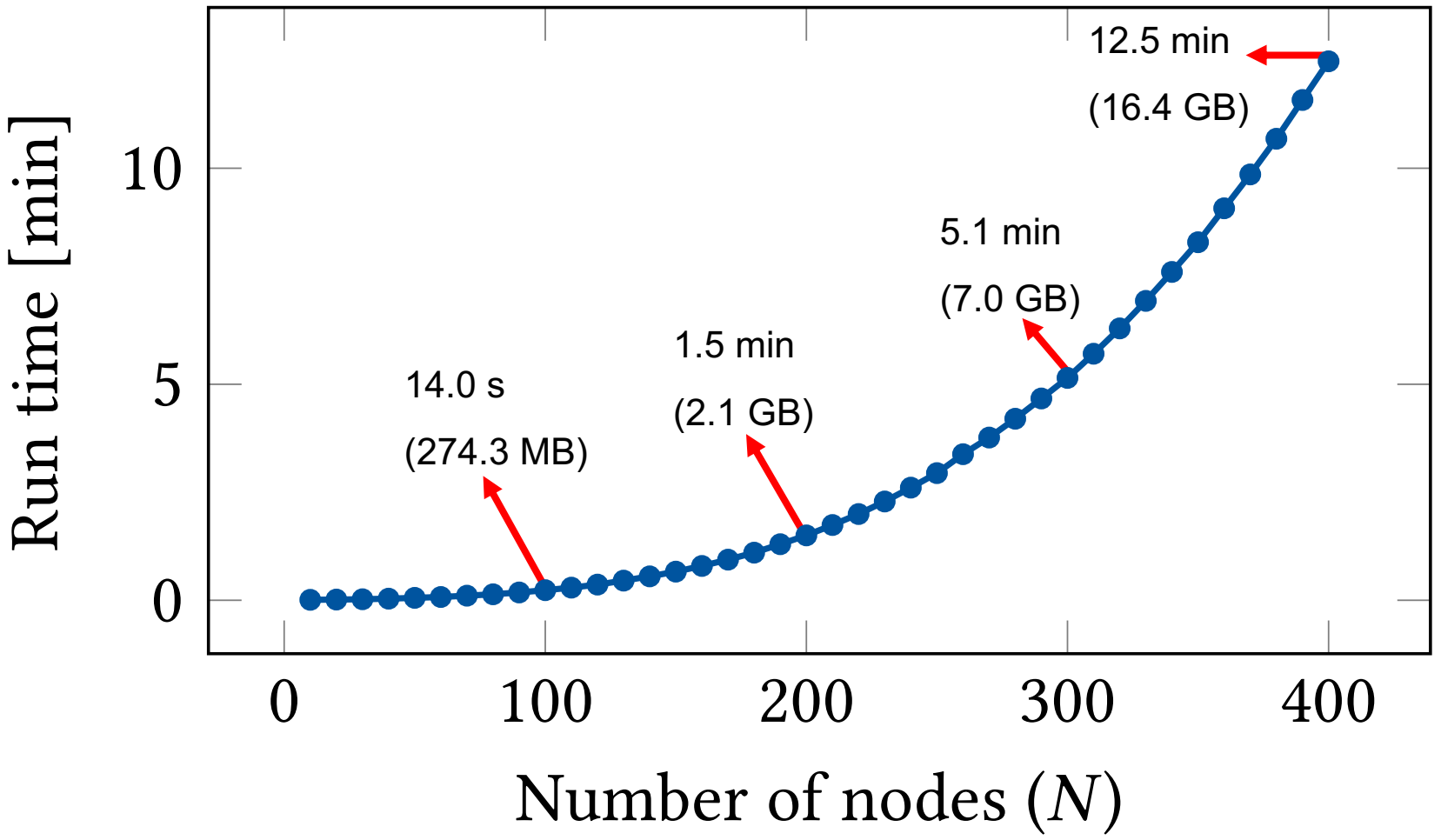
- Implementation in MP-SPDZ [Kel20]
- Three parties
- Replicated Secret Sharing [AFLNO16] (passive security)
- LAN setting: 1Gbit, 1ms RTT



[AFLNO16] T. Araki, J. Furukawa, Y. Lindell, A. Nof, and K. Ohara. **High Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority.** In ACM CCS, 2016.

[Kel20] M. Keller. **MP-SPDZ: A Versatile Framework for Multi-Party Computation.** In ACM CCS, 2020.

Results II


Run time [min]
10
5
0
0
100
200
300
400
Number of nodes (N)
12.5 min
(16.4 GB)
5.1 min
(7.0 GB)
1.5 min
(2.1 GB)
14.0 s
(274.3 MB)

Thank you for your attention!

Paper (Full Version): https://eprint.iacr.org/2022/1173

Contact: https://encrypto.de/brueggemann

References

[AFLNO16] T. Araki, J. Furukawa, Y. Lindell, A. Nof, and K. Ohara. **High Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority.** In ACM CCS, 2016.

[Avi83] D. Avis. **A Survey of Heuristics for the Weighted Matching Problem.** In Networks (13), 1983.

[BMW22] M. Breuer, U. Meyer, and S. Wetzel. **Privacy-Preserving Maximum Matching on General Graphs and its Application to Enable Privacy-Preserving Kidney Exchange.** In ACM CODASPY, 2022.

[BS15] M. Blanton and S. Saraph. **Oblivious Maximum Bipartite Matching Size Algorithm with Applications to Secure Fingerprint Identification.** In ESORICS, 2015.

[DES16] J. Doerner, D. Evans, and a. shelat. **Secure Stable Matching at Scale.** In ACM CCS, 2016.

[Kel20] M. Keller. **MP-SPDZ: A Versatile Framework for Multi-Party Computation.** In ACM CCS, 2020.

[Pre99] R. Preis. **Linear Time 1/2-Approximation Algorithm for Maximum Weighted Matching in General Graphs.** In STACS, 1999.