Student: Danila Romanov (4835786)
Responsible Professor: Dr. Zekeriya Erkin
Teacher Assistant: Tianyu Li

CSE3000 01/07/2021

How can multiple firms collaborate in the supply chain without revealing data?

Delft University of Technology

Research Question

"How can secure multiparty computation be used to preserve privacy in supply chain collaboration"

Introduction:

- Supply chain collaboration
  - Companies benefit (e.g reducing costs or time)
  - Example is logistics (such as sharing trucks)
- Company data should not be shared because
  - It can be used to give competitors an advantage
- Trusted third parties can be used as mediators
  - Can they be trusted?
  - They add costs
  - Can we do it without?
- Secure Multiparty Computation (MPC)
  - Computes a function in a distributed manner
  - Doesn't reveal information to other parties
  - Adversarial model
    - Semi-honest has weaker privacy
    - Malicious model is too inefficient

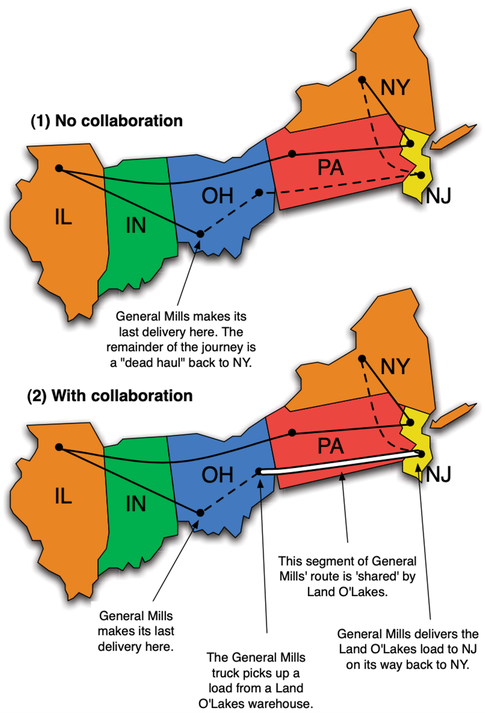


Figure 1: A logistics supply chain problem

Method

- Literary review on privacy preserving collaboration
- Which collaboration problems can secure multiparty computation solve?
- Which supply chain problems can they be used in?
- To what extent does it protect privacy?

Collaborative Optimization Research

- To solve supply chain problems we use collaborative optimization research
- MPC is used in here to preserve privacy
- Collaborative problems
  - Travelling Salesman Problem
  - Linear Programming
  - Graph Coloring
  - Constraint Satisfaction Problem

Table 1: Overview of collaboration research solved using MPC and its application in a supply chain collaboration problem

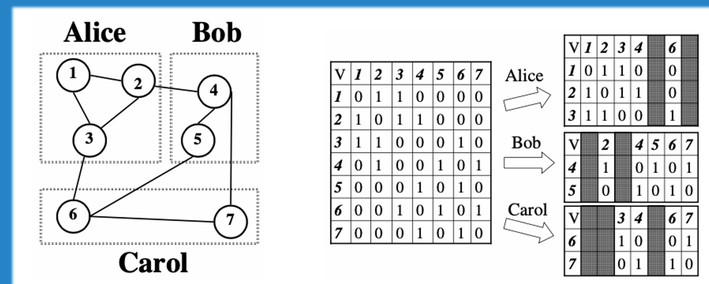
Supply chain problem	Optimization problem	Notes	Source
Collaborative Transport and Production	Linear Programming	Possible inference attacks	Hong, 2012; Hong, 2016
Distributed Scheduling and Network Allocation	Graph coloring	Minor privacy leakage	Hong, 2018
Vehicle Routing	Traveling Salesman Problem	No issues	Hong, 2014
Resource allocation and planning	Constraint Satisfaction	Modified MPC that preserves both constraints and decisions	Leaute, 2009
Capacity Sharing and Price-masking	Other	No issues	Clifton, 2008; Deshpande, 2011

Important Results

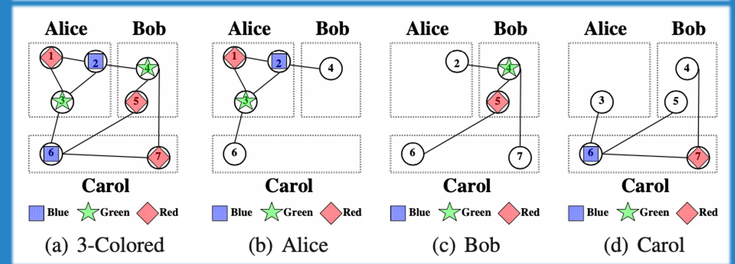
- MPC in the semi-honest model is most used
- This lacks privacy against malicious parties
- MPC is inadequate at verifying if parties lie in private input
- To solve, combine MPC with game theory
  - Game theory is mathematical study of strategic interaction
    - Rational decision-makers
  - Incentive compatibility
    - Best interest of parties to be honest
    - Else they lose benefits or are caught

Conclusion

- MPC has various applications to supply chain collaboration
- Incentive compatible semi-honest protocols have potential
  - Improves practicality
  - More research should be performed



(a) Partitioned Graph (b) Partitioned Adjacency Matrix



(a) 3-Colored (b) Alice (c) Bob (d) Carol

Figure 2: Graph coloring used to solve a job scheduling problem (Hong, 2018)

References

A.Bednarz, Methods for two-party privacy-preserving linear programming. PhD thesis, 2012.
C. Clifton, A. Iyer, R. Cho, W. Jiang, M. Kantarcıoglu, and J. Vaidya, "An approach to se- curely identifying beneficial collaboration in decentralized logistics systems,"
V. Deshpande, L. B. Schwarz, M. J. Atallah, M. Blanton, and K. B. Frikken, "Outsourcing manufacturing: Secure price-masking mechanisms for purchasing component parts," *Produc- tion and Operations Management*, vol. 20, no. 2, pp. 165–180, 2011.
Manufacturing & Service Operations Management, vol. 10, no. 1, pp. 108–125, 2008.
Y. Hong, J. Vaidya, N. Rizzo, and Q. Liu, "Privacy-preserving linear programming," in *WORLD SCIENTIFIC REFERENCE ON INNOVATION: Volume 4: Innovation in Information Security*, pp. 71–93, World Scientific, 2018.
Y. Hong, J. Vaidya, and H. Lu, "Secure and efficient distributed linear programming," *Journal of Computer Security*, vol. 20, no. 5, pp. 583–634, 2012.
Y. Hong, J. Vaidya, and H. Lu, "Securely solving the distributed graph coloring problem," 2018.
Y. Hong, J. Vaidya, H. Lu, and L. Wang, "Collaboratively solving the traveling salesman prob- lem with limited disclosure," in *Data and Applications Security and Privacy XXVIII* (V. Atluri and G. Pernul, eds.), (Berlin, Heidelberg), pp. 179–194, Springer Berlin Heidelberg, 2014.
T. Leaute and B. Faltings, "Privacy-preserving multi-agent constraint satisfaction," in *2009 International*