A Survey on the Privacy-Preserving Applications of Secure Transformation in Collaborative Supply Chains

Andrei-Alexandru Stefan (4839870), Zekeriya Erkin, Tianyu Li

TU Delft

CSE3000

1 July 2021

1. INTRODUCTION

- Supply chain – complex network composed of suppliers, manufacturers, retailers, and customers
- Collaborative supply chain – two or more participants collaborate
- Solving the problem requires knowing all the information
- Collaborators have private data
- Privacy-preserving techniques: secure multiparty computation (MPC) and secure transformation (ST)

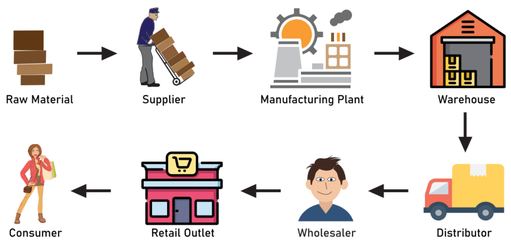

Figure 1: Traditional supply chain [1]

OBJECTIVES

- **Main research question: "How do secure transformation applications preserve privacy in collaborative supply chains?"**
- Find out how MPC and ST work
- Find advantages and disadvantages of each approach
- Discuss feasibility for real-life applications

2. METHOD

- Literature review of privacy-preserving collaborative techniques
- Present the general form of a transformation
- Explain how ST solves problems
- Consider if it is good enough for real-life applications

3. RESULTS

PROBLEM STATEMENT

- The optimal solution is the output of a function with multiple inputs
- Collaborators try to find the solution, **without** revealing private information
- Besides the function: variables, and constraints

A GENERIC TRANSFORMATION

$$\begin{aligned} \min\ & c^T\mathbf{x} \\ s.t.\ & M\mathbf{x} \geq B \\ & \mathbf{x} \geq 0 \end{aligned} \longrightarrow \begin{aligned} \min\ & c^T Q Q^{-1}\mathbf{x} \\ s.t.\ & MQQ^{-1}\mathbf{x} \geq B \\ & Q^{-1}\mathbf{x} \geq 0 \end{aligned}$$

[2]

- $MQ = M'$, $Q^{-1}x = y$, and $c^TQ = c'^T$, with Q an invertible matrix
- x is a vector of variables
- c is a vector of objective function coefficients
- M is a matrix of constraint coefficients
- B is a vector of constraint values

SECURE TRANSFORMATION

- Relies on transforming the input and the problem
- Result to the original problem found by inverting the transformation [3]
- Usually solves linear programming problems
- Advantage: tailor made transformation to solve a certain problem, fast
- Disadvantage: only heuristic security in most cases [2], non-cryptographic
- Recent developments: revised older transformations; pointed out issues; proved impossibility outside of finite fields [4]; showed usefulness in outsourcing to the cloud

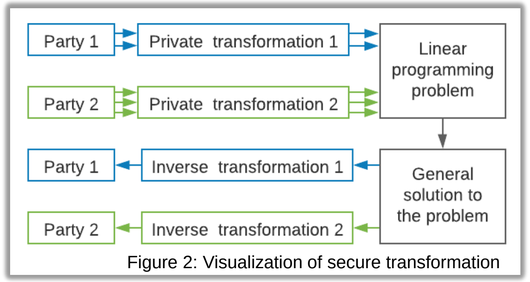

Figure 2: Visualization of secure transformation

IS ST USEFUL FOR REAL-LIFE APLLICATIONS?

- Collaborative Scheduling and Routing: can be used in last mile delivery and bin packing
- Collaborative Container Maritime Logistics: can be used in several optimization problems, such as optimizing container handling time
- Collaborative Airline Management: can be used in schedule design

4. CONCLUSIONS

- Developments for specific cases of linear programming problems
- Faster than cryptographic methods, but provides less security guarantees [4]
- Possibilities for using secure transformation in supply chain applications, theoretically
- Possibilities in computation outsourcing to cloud
- Not deployed in practice yet

LIMITATIONS

- Security is mostly heuristic [2]
- Perfect secrecy impossible when not working in a finite field [4]
- More research is needs to be conducted

REFERENCES

[1] V. Hassija, V. Chamola, V. Gupta, S. Jain, and N. Guizani, "A survey on supply chain security: Application areas, security threats, and solution architectures,"IEEE Internet of Things Journal, vol. 8, no. 8, 2020

[2] Y. Hong, J. Vaidya, N. Rizzo, and Q. Liu, "Privacy preserving linear programming," CoRR, vol. abs/1610.02339, 2016

[3] W. Du, A study of several specific secure two-party computation problems. PhD thesis, Purdue University, 2001

[4] A. Pankova and P. Laud, "Transformation-based computation and impossibility results," in Applications of Secure Multiparty Computation, pp. 216–245, IOSPress, 2015

CONTACT

Andrei-Alexandru Stefan

A.A.Stefan@student.tudelft.nl