Research Center
Finance & Information Management

Fraunhofer
FIT

Project Group
Business & Information
Systems Engineering

Discussion Paper

Supply Chain Network Risk Analysis - A Privacy Preserving Approach

by

Gilbert Fridgen, Tirazheh Zare Garizy

in: Proceedings of the 23rd European Conference on Information Systems (ECIS),
Münster, Germany, May 2015

WI-480

University of Augsburg, D-86135 Augsburg
Visitors: Universitätsstr. 12, 86159 Augsburg
Phone: +49 821 598-4801 (Fax: -4899)

University of Bayreuth, D-95440 Bayreuth
Visitors: F.-v.-Schiller-Str. 2a, 95444 Bayreuth
Phone: +49 921 55-4710 (Fax: -844710)

www.fim-rc.de

SUPPLY CHAIN NETWORK RISK ANALYSIS A PRIVACY PRESERVING APPROACH[1]

Complete Research

Fridgen, Gilbert, FIM Research Center, University of Bayreuth, Friedrich-von-Schiller-Str. 2a, 95444 Bayreuth, Germany, gilbert.fridgen@fim-rc.de

Zare Garizy, Tirazheh, FIM Research Center, University of Augsburg, Universitaetsstrasse 12, 86159 Augsburg, Germany, tirazheh.zare-garizy@fim-rc.de

Abstract

Globalization and outsourcing are two main factors which are leading to higher complexity of supply chain networks. Today's complex distributed supply chain networks are vulnerable to various kinds of risks. Due to the strategic importance of having a sustainable network it is necessary to have an enhanced supply chain network risk management. The first step in the risk management is risk identification. In a supply chain network many firms depend directly or indirectly on a specific supplier. Any failure in a supplier's production can risk the whole network's robustness. In this regard, unknown risks of network's structure can endanger the whole network's robustness. In spite of the importance of risk identification of supply chain network, companies are not willing to exchange the structural information of their network. Firms are concerned about risking their strategic positioning or established connections in the network. Combining the secure multiparty computation cryptography methods with risk identification algorithms driven from social network analysis, is the solution of this paper for this challenge. With this combination we enable structural risk identification of supply chain networks without endangering companies' competitive advantage.

Keywords: Supply Chain Network, Risk Management, Multiparty Computation, Algorithms, Privacy.

[1] This research was in part carried out in the context of the Project Group Business and Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT.
Grateful acknowledgement is due to the DFG (German Research Foundation) for their support of the project „ITPM (FR 2987/2-1, BU 809/13-1)" making this paper possible.

1 INTRODUCTION

In March 2000, a thunderstorm in New Mexico has caused a 400-million-dollar loss for the telecommunications equipment company Ericsson. The fire in a semiconductor plant, a single source key components provider for Ericsson, led to this damage. This loss could have been lower with an appropriate risk management within the supply chain network (SCN) of Ericsson (Peck 2003).

Higher complexity of SCNs and steady increase in vulnerability within the SCN are the results of globalization and outsourcing. The globalization of sourcing networks, customer or supplier dependencies, and the supply chain complexity (Wagner and Neshat 2012) are important drivers of SCNs risk. 54% of companies are either extremely or very concerned about their sustainability performance (HBR Advisory Council 2010). Being one of the four emerging issues in global risk (Emmerson et al. 2008), it is inevitable to invest in risk management for supply chains. Managers and public policy makers need to identify risks to perform proper risk management and mitigation plans.

Simulation models (Fridgen et al. 2014; Giannakis and Louis 2011; Chu et al. 2010), descriptive case studies (Blome and Schoenherr 2011; Choi and Hong 2002), and development of taxonomies of SCNs (Miemczyk et al. 2012; Zhao et al. 2010) are common research results of the scholars on analysis of SCNs. The embedded positioning of firms within the SCN is important for each firm in the network as well as for the network as a whole. Innovation adoption, influence power or brokering activities of the firms can be derived from their structural positioning in the SCN. Moreover the structural positioning of the firms can affect the vulnerability or robustness of the SCN (Kim et al. 2011). Over the last few decades, the importance of adopting a network perspective in supply chain analysis and management has increased. Recently, the idea of adopting network measures for the investigation of SCNs is opening new potentials to evaluate supply chains (Vereecke et al. 2006; Kim et al. 2011; Mizgier et al. 2013).

There are several measures to quantitatively characterize the network structure. Each measure can be adopted to capture a specific feature of the network (Newman 2010). Betweenness, closeness, and degree centrality are some of the widely used measures in social network analysis (Wasserman and Faust 1994; Freeman 1977). Kim et al. (2011) mapped these measures within the SCN and defined their implication for two types of supply networks: material flows and contractual relationships. They identified that firms with higher betweenness centrality (BC) have a higher impact on the product quality, coordination cost, and lead time or can cause unwanted intervene or control among the SCN. The BC is an indicator for identifying firms with the possibility of influencing information processing, strategic alignments, and perverting risk management within the supply network (Kim et al. 2011). Based on Hallikas et al. (2004) the risks in a SCN can affect the long-term sustainable competitive advantage of the network. Considering our focus and above mentioned findings, we assume the BC to be an appropriate measure to identify risk in the SCN.

One of the main challenges in studying supply chain risks is the scarcity of real life data on SCNs (Kim et al. 2011; Kersten et al. 2008). The fear of risking competitors' advantage by information sharing hinders companies' collaboration within the SCN. To calculate the BC, either based on definition (Freeman 1977; Newman 2010), or by means of widely used algorithms such as Brandes' (2001), having information about the network's structure is necessary. This structural information contains data on the network's firms and their possible connectivity to other firms. However, the strategic importance of the firms' position and connections within the network (Hochberg et al. 2007) dissuades firms from sharing this information. In this case, the application of secure multiparty computation (SMC) cryptographic algorithms (Yao 1986; Goldreich et al. 1987) would be one of the solutions to facilitate information sharing willingness within the network. SMC algorithms are based on simultaneous exchanges of encrypted data among parties. The result is calculated from the encrypted data, and is shared among all firms (parties) in the network. The algorithm prevents leakage of key information between the firms.

Given the importance of risk analysis in SCNs and the adequacy of the BC to identify the bottlenecks in SCNs, the main focus of this paper is to introduce an artifact – based on the design science paradigm – for privacy preserving calculation of the BC of a given SCN. Our artifact consists of four main methods that are calculating the desired result. The main contributions of our paper are:

- Identification of risks: In the first step of risk management it is necessary to develop models and methods for risk identification in SCNs. In a small SCN, companies are more likely to keep the overview of the SCN topology and the companies in the network. Consequently, in such cases risks are relatively transparent and privacy is not the subject of interest. Our concern is the risk identification in large SCNs consisting of hundreds of inter-connected companies. In a large SCN, on the one hand the identification of unknown risks is important and on the other hand the privacy of members should be maintained. For an increasing size of the SCN and the inter-relationships among the firms, the network becomes more complex (Choi and Krause 2006). Due to the higher complexity the probability of unseen risks and the necessity of proper risk analysis increases. In the artifact proposed, we study the economic dependency (e.g. material or financial flow) between firms by means of BC calculation for the identification of risks in SCNs. We thereby assume that our artifact could be a module of standard ERP systems that use existing communication links to suppliers and customers.
- Preservation of Privacy: One of the main concerns of companies in a SCN is their strategic position in the network, so they avoid to risk their competitive advantage in order to identify their own risks. Our artifact keeps the network's structure mostly unknown to the firms within the network. The artifact prevents data leakage or reconstruction of information to ensure the firms' willingness for information sharing. In order to meet this objective, we base our approach on SMC algorithms in a semi-honest environment as outlined in the latter. Our modeling focus is on providing a privacy preserving artifact, whereas we omit the analysis and improvement of computational complexity.

Considering the guidelines of Hevner et al. (2004) and Gregor and Hevner (2013) for the conduction of design science research, the remainder of this papers is organized as follows: The first section covers a brief review on essential literature. It also includes specifying the problem's context and the relevance of the problem for SCNs. Subsequently, we discuss the modeling procedure and requirements that must be met for solving the problem. The fourth section illustrates the developed artifact. The section is followed by the evaluation of the artifact by means of testing and descriptive methods. The paper ends with a summary and an outlook on further research.

2 LITERATURE REVIEW

2.1 Supply Chain Networks

"Supply chains are interlinked networks of suppliers, manufacturers, distributors and customers that provide a product or service to customers" (Blackhurst et al. 2004). Current trends, like e-commerce, e-logistics, and e-business, increase the complexity of supply chains. Furthermore, the importance of staying competitive in the market gives supply chain management a higher importance (Arns et al. 2002). The SCN in a global economy consists of a large number of interdependent networks. This interdependency is very susceptible to external effects and defaults (Buhl and Penzel 2010). The risk type in SCNs can be specific disruption, general disruption, cost shock (e.g. exchange rates), product safety, commoditization, and shift in tastes (Lessard 2013). Weather, terrorism, firms manufacturing failures, or financial crises can cause a default in the supply chain (Babich et al. 2007). Risks in SCNs can lead to various types of losses such as financial loss, performance loss, physical loss, psychological loss, social loss and time loss (Yate and Stone 1992). Since the disruptions in SCN in extreme cases may lead to the bankruptcy of the SCN's firms, it is important for the firms to manage these risks and minimize the possible losses. A study of Gyorey et al. (2011) shows that 67% of companies are not ready for geopolitical instability challenges. In the management of SCNs, one of the main tasks is risk management. The risk management process consists of risk identification and assessment, decision and implementation of risk management actions, and risk monitoring (Hallikas et al. 2004). Bellamy and Basole (2013) classified the themes in SCNs analysis as system architecture (network structure), system behavior, and system policy and control. Among these categories, system architecture analysis methods focus on structural investigation of SCNs, relationship of firms, and the importance of the relationship. Considering social networks, structural investigations based on network analysis methods are well-established. In the field of SCNs they are relatively new but evolving (Li and Choi 2009; Kim et al. 2011; Mizgier et al. 2013). These methods focus on network components' connections and patterns, and implication of these connections for the whole network (Wasserman and Faust 1994; Newman 2010). Among various measures on structural analysis of SCN, as it has been mentioned earlier, the BC can be a suitable indicator to identify the structural risks of a SCN (Kim et al. 2011) and it is our choice in this paper.

2.2 Privacy Concerns in Supply Chain Networks

On the one hand knowing the structure of a network is a prerequisite of calculating the BC (as outlined earlier) and on the other hand in a SCN, the competitive advantage of network firms is relying on the privacy of their contacts and network relations they have (Buhl and Penzel 2010). Solutions to these data privacy concerns of companies can be:

- A Trusted Third Party: If the firms trust a third party, it is easy to solve the problem by sharing their information with this trusted third party and letting it calculate the results. For instance, Brandes' algorithm for the BC (2001), works based on the idea of having a third party who collects the information and calculates the indices and returns the result. In practice such a party that all network's firms trust might be difficult to find and firms might have concerns about this third party revealing the information.
- SMC Algorithms: These cryptography algorithms enable different firms in the network to share their information privately and calculate the result jointly. The main advantage of these algorithms is that the individual's input stays mostly private.

SMC first was addressed by Yao (1982). Yao's algorithm is answering the question of SMC for two parties. This algorithm is a solution to the Millionaires' problem. The problem is that two millionaires want to know which of them is richer but they do not want to share the real amount of their wealth. Yao's algorithm provides a solution that lets them privately encrypt their input, share it, and jointly calculate the result. The main advantage is that their input stays private. SMC algorithms today enable us to do secure addition, multiplication, and comparison (Shamir 1976; Yao 1986; Sheikh et al. 2009; Cramer et al. 2013).

SMC algorithms are used in various fields of science. For instance they are used for secure auctions (Bogetoft 2006). They are also used for sharing financial risk exposures (Abbe et al. 2012) with the focus on necessity of process and methods secrecy in financial industry. SMC algorithms are also applied for sustainable benchmarking in clouds without disclosing the individual's confidential information (Kerschbaum 2011).

"SecureSCM", secure collaborative supply chain management, the European research project (Kerschbaum et al. 2011), is an example of the application of SMC algorithms in the field of SCNs. The project enabled privacy preserving online collaboration among various firms in a SCN. The focus was on providing the possibility to better reaction on possible capacity concerns or short notices. The collaboration of the firms with the application of SMC algorithms results in better production planning in the SCN. However, they did not study SCN's risks and focused on cost minimization.

In this paper, SMC algorithms are our choice for the privacy preserving calculation of the result. To apply these algorithms, we develop an artifact that enables calculation of the result based on private shares of firms. SMC algorithms have a high acceptance and are widely used in the field of cryptography since the 1980's (Dolev and Yao, 1983; Beaver et al. 1990; Lindell and Pinkas, 2009; Bogetoft et al. 2006; Reistad, 2012). Therefore, we do not investigate the security of these algorithms and assume security is given.

2.3 Network Centrality Measures

To calculate the BC, we model the SCN as a graph $G(V, E)$. Each company v in the SCN is represented by a vertex $v \in V$. An economic dependency (e.g. material or financial flow) between companies $u, v \in V$ is represented by an edge $(u, v) \in E$ between these companies. In this case, we name u and v adjacent or neighbors. Since an economic dependency is undirected, in this paper graphs are undirected. Moreover the graphs are connected, as connected firms are forming a SCN. The BC is a centrality index based on the number of shortest paths and the frequency in which a vertex is appearing on shortest paths between two other vertices. The shortest path is a path between two vertices such that the sum of the weights of its constituent edges is minimized (as outlined in Modeling section). The BC describes how other vertices potentially can influence the interaction between two non-neighboring vertices (Wasserman and Faust 1994; Newman 2010). Based on Newman (2010) the BC for vertex v is calculated as follows:

$$BC(v) = \sum_{s \neq v \neq t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}} \qquad (1)$$

In Equation (1), $\sigma_{st}(v) \in \mathbb{N}_0$ is the number of shortest paths between source vertex s and target vertex t, which pass through vertex v, and σ_{st} is the number of shortest paths between source vertex s and target vertex t.

The main aspect of the BC algorithms (Jacob et al. 2005; Klein 2010; Brandes 2001) is finding the shortest paths. Based on categorization of Cormen et al.'s (2001) on shortest paths algorithms we classify existing BC algorithms as follows:

- Algorithms based on single-source shortest paths: Brandes' (2001) algorithm is a widely used one among them. Brandes applies single source shortest paths algorithms (breadth-first (Moore 1959)) search for unweighted and Dijkstra's algorithm for weighted graphs (Dijkstra 1959; Cormen et al. 2001)) to calculate the BC.
- Algorithms based on all-pairs shortest paths: The method developed by Edmonds et al. (2010) adopted modification of algorithms like the Floyd-Warshall (Floyd 1962; Warshall 1962; Cormen et al. 2001) to enable parallelism and space-efficiency in calculation of the BC.

Both categories of algorithms need the network topology as input and a stack to store information. For privacy concerns we strive to avoid a central stack for information. Having a central stack implies that there is a central player who owns this stack. This player can infer information, from the communication of the players via this stack or from the large amounts of available data (although the information is encrypted) in the stack. This can be a risk for privacy concerns of the firms in the SCN.

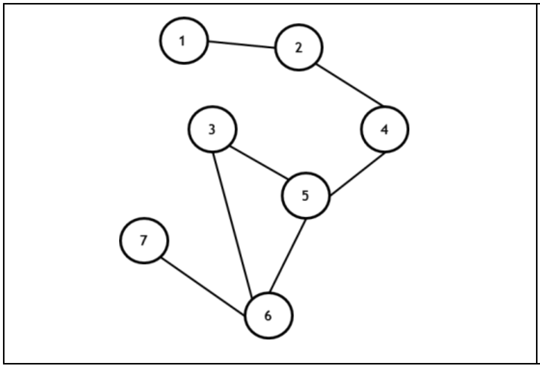
In this paper, inspired by the Floyd-Warshall algorithm as well as backtracking search (Russel and Norvig 2009) to identify shortest paths, we develop an artifact which does not need a central stack, stores information decentrally, and does not need the network's topology as input.

3 Modeling Procedure, Assumptions, and Requirements

The first part of this section focuses on modelling procedure and assumptions for our artifact. In this part before we focus on privacy concerns and information that each firm has, we define the general terms and construct of our artifact. The second part includes the more specific information on privacy preserving of the firms and requirements.

We label each company and its representing vertex with a unique number $1,2, \ldots, |V|$. The numbers are randomly assigned to each company and represent the row number for the player in the graph's weight matrix. The relation between the identity of a company and its number is only known to the company itself and to the neighboring companies. From now on, we name a company and its representing vertex as a "player" when we mean the company's row number and not the true identity of the company. We assume that $|V| = n$, the number of companies in a SCN, is given.

In the following, we illustrate an exemplary SCN (Figure 1). The SCN is chosen simple to make the visualization easier and the example more comprehensible. The SCN consists of 7 players. Each player is represented by its own unique number. The set of vertices (players) is: $V = \{1,2,3,4,5,6,7\}$.



$$W = \begin{bmatrix} 0 & 1 & \infty & \infty & \infty & \infty & \infty \\ 1 & 0 & \infty & 1 & \infty & \infty & \infty \\ \infty & \infty & 0 & \infty & 1 & 1 & \infty \\ \infty & 1 & \infty & 0 & 1 & \infty & \infty \\ \infty & \infty & 1 & 1 & 0 & 1 & \infty \\ \infty & \infty & 1 & 0 & 1 & 0 & 1 \\ \infty & \infty & \infty & \infty & \infty & 1 & 0 \end{bmatrix}$$

Figure 1. Exemplary network

For reasons of simplicity, the following assumptions are the basis for the development of our artifact.

Assumption 1. *The companies are semi-honest (honest-but-curious).*

Semi-honest adversaries are following the protocol, but they might try to gather information and draw conclusions from the messages they receive. Our artifact's construction preserves privacy assuming the companies are semi-honest. Moreover, related works on SMC algorithms are also based on a semi-honest model (Brickell and Shmatikov 2005; Canetti 2008; Huang et al. 2012; Schneider 2012).

Assumption 2. *The connections in the SCN are equally weighted.*

In general, our artifact is applicable for graphs with $w_{uv} \in \mathbb{R}$. However, Kim et al. (2011) did their analysis on the BC, assuming equal weight connections. Their focus is on links between firms and the number of firms that are engaged in transferring information or material. Therefore, without loss of generality, in this paper we do not focus on the determination of the intensity of connections and its analysis and we treat the connections as equally weighted and leave the topic of connections' intensity subject to further research. The weight of the edge $(u, v) \in E$ with arbitrary $u, v \in V$ is then defined by

$$w_{uv} = \begin{cases} 0 & if\ u = v, \\ 1 & if\ u \neq v\ and\ (u, v) \in E, \\ \infty & if\ u \neq v\ and\ (u, v) \notin E. \end{cases} \tag{2}$$

The $n \times n$ matrix $W = (w_{uv})$ contains all weights of edges in the graph $\forall\, u, v\ \in V$ (Cormen et al. 2001). The (symmetric) matrix W in Figure 1 represents the weight matrix of our exemplary SCN.

The sequence of vertices that are forming the path from a source vertex $s \in V$ to a target vertex $t \in$ V is represented by $path = \langle v_0, v_1, \dots, v_k \rangle$. In this we assume that $v_0 = s$, $v_k = t$, and $(v_{i-1}, v_i) \in E$ for $i = 1\ to\ k$. The length of the path is the sum of the weights of its forming edges. Based on Equation (2) the weight of an edge is 1 therefore, if k vertices are forming a path, there are $k - 1$ edges on this path and $w(path) = k - 1$. We define the length of the shortest path, labeled as distance between s and t, as

$$d_{st} = \min\{w(path): v_s \overset{path}{\leadsto} v_t\}. \tag{3}$$

The $n \times n$ matrix $D = (d_{st})$ contains the distances $\forall\, s, t\ \in V$. By our definition, if s and t are adjacent then $d_{st} = 1$. To find the shortest path from a source vertex s to the target vertex t, the existing distance and the distance of all alternative paths via intermediate vertices $\forall v \in V, v \neq s, t$ are compared (Equation (4)) and we choose the path with the minimum length.

$$\min(d_{st}, d_{sv} + d_{vt}) \tag{4}$$

In this part we represent the above mentioned figures with particular details which include privacy preserving concerns and information availability for the players.

In our artifact we restricted the information availability of the players mostly up to their neighbors. Therefore, although the set V is known for every player in the network, but the relation between the players' unique numbers and their true identities is in only known for neighboring players. Furthermore the network's structure as illustrated in the Figure 1 is not known for the players. Consequently W is unknown for the players. Each player p has access to the $p-th$ row (or column, since the matrix is symmetric) of the weight matrix W. The accessible information for player 5, is the 5-th row of the matrix, as marked in the Figure 1. Moreover the distance matrix D is unknown to the players. Although, each player p has access to the p-th row of the matrix D.

For our artifact we state the following requirements:

Requirement 1. *The artifact should keep the SCN topology as private as possible.*

Requirement 1 is an extension to conditions of SMC on satisfying privacy (Cramer et al. 2013). In our case it is allowed that more information than the final result (BC) is shared. More specifically, we prohibit the sharing of the following information that can be used for reconstructing the SCN topology or interfering the real identity of the firms.

- The length of the shortest paths, to prevent firms from knowing the positioning of the players in the network.
- The number of the shortest paths between a given source and target player in the network, to prevent firms from knowing which alternatives for trading players have in the network.
- The number which shows how often a player is appearing on the shortest paths between a given source and target player, to prevent firms from knowing accessibility and connections to other firms.

Requirement 2. *The artifact should keep the identities of non-neighboring players private.*

In a large SCN, due to members' variety and multiplicity in the SCN, a company is not able to identify other companies in the network. Concluding the identity of a player via execution of the artifact can provide the possibility of reconstructing a part of the network's topology. Therefore, the artifact should not enable a company to infer the real identity of non-neighboring companies.

4 Artifact Development

We chose an object oriented approach for elaboration of our artifact. To model the structure and behavior of the players in our artifact we define the class Player. We represent each player by an object of the class Player running on a distributed system. Each player executes methods privately and independently from other players. The methods of a player can be called by other players, but each player executes a method on its own system and delivers the result. In our artifact we assume there is an initializing and synchronizing agent (ISA) (one of the SCN's firms or an organization) who initializes, coordinates, and synchronizes the executions. The ISA does not have the possibility to access the private information of the players or monitor the communication between the players.

Figure 2 presents the Player class. For reasons of simplicity, in the following we assume the players' object references to equal their respective $rowNumber$ during the calculations. $rowNumber$ is a unique number assigned to each player in the network. $rowNumber = p$ implies the player is pointing the p-th row of the weight matrix W.

We assume p is the number of the current object of the Player class. Table 1 provides the description of the attributes of the Player class. Table 2 provides the description of the methods of the Player class.

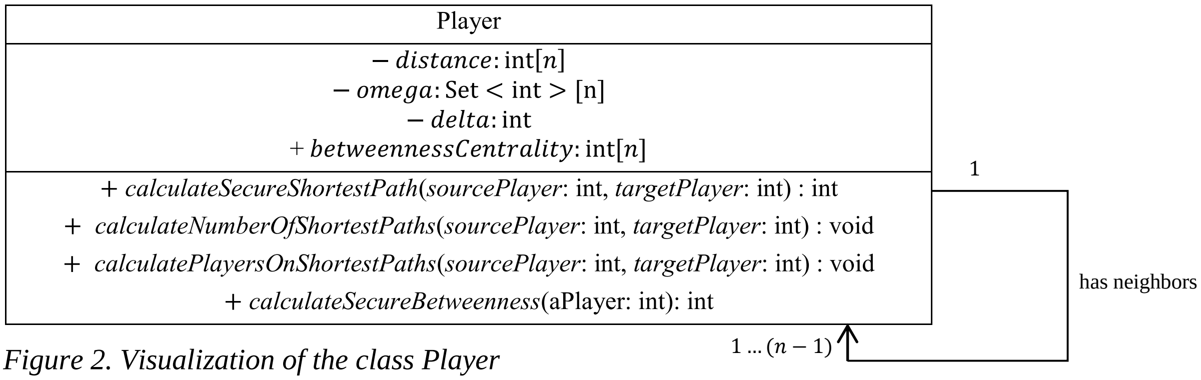

Player
$-\,distance$: int$[n]$
$-\,omega$: Set $<$ int $>$ [n]
$-\,delta$: int
$+\,betweennessCentrality$: int$[n]$
+ *calculateSecureShortestPath*(*sourcePlayer*: int, *targetPlayer*: int) : int
+ *calculateNumberOfShortestPaths*(*sourcePlayer*: int, *targetPlayer*: int) : void
+ *calculatePlayersOnShortestPaths*(*sourcePlayer*: int, *targetPlayer*: int) : void
+ *calculateSecureBetweenness*(aPlayer: int): int
1
has neighbors
$1 \dots (n-1)$

Figure 2. Visualization of the class Player

Attribute	**Mathematical Variable**	**Description**
$distance$: int$[n]$	$D = (d_t)$ $\forall\, t \in V$	Denotes the vector which is filled with the distances of player p to all vertices in the network.
$omega$: Set $<$ int $>$ [n]	$\Omega = (\Omega_t)$ $\forall\, t \in V$	Denotes the vector which contains the set of neighboring players of player p that are connecting the player with the shortest path to the target player t. Members of Ω_t are described by ω.
$delta$: int	δ	Denotes a random generated number of the player. We use it to modify the distance value to preserve privacy.
$betweennessCentrality$: int$[n]$	$BC = (BC(v))$ $\forall\, v \in V$	Denotes the vector which is filled with the BC of all players in the network.

Table 1. Description of the attributes of the Player class

Method	**Description**
Name: *calculateSecureShortestPath*() Input: *sourcePlayer*: int, t*argetPlayer*: int Output: distance: int	The method recursively identifies the shortest paths from the given source player to the given target player. It returns the encrypted value of the distance and keeps other variables local. If the target player is not the current player, *calculateSecureShortestPath*() method calls itself at all neighboring players to determine their distances to the target. The method compares the delivered results from neighboring players and chooses the path via the neighboring player/s which is/are delivering the minimum distance value. Source player s is an input variable to ensure assignment of the values takes place only when the method returns to the source player who started the query. For privacy preserving purposes the comparisons in this method is based on Yao's (1982) secure comparison protocol. The method also identifies the neighboring players who are forming the shortest paths and fills Ω.
Name*: calculateNumberOfShortestPaths*() Input: *sourcePlayer*: int, *targetPlayer*: int Output: void	The method recursively calculates the *number* of the shortest paths between the source player and each given target t in the network. If the target player is not a neighboring player of the source player, *calculateNumberOfShortestPaths*() method calls itself for all neighboring players. The source and target are input variables to ensure players are updating the value of σ_{st}^{p} (player p's part of information on σ_{st}) for the desired source and target. The size of set Ω_t provides the information to calculate the number of shortest paths.

Method	Description
Name: *calculatePlayersOnShortestPaths*() Input: *sourcePlayer*: int, *targetPlayer*: int Output: void	The method recursively calculates how often players (who are forming the shortest path(s)) are appearing on the shortest path(s) from source player s to target player t. If the target player is not a neighboring player of the source player, the method calls itself for all neighboring players. It recursively determines which players are connecting source player s and target player t with the shortest path. The source and target are input variables to ensure players are updating the value of $\sigma_{st}^{p}(v)$ (player p's part of information on $\sigma_{st}(v)$) for the specific source and target. The members of set Ω_t as well as the size of the set, provides the necessary information for the calculation.
Name: *calculateSecureBetweenness*() Input: *aPlayer*: int Output: BC(v): int	This method calculates the $\mathrm{BC}(v)$ for the given player in the network. It is based on SMC algorithms and simultaneously exchanges information among the players in the network. The method performs all arithmetic based on secure protocols of Cramer et al. (2013). These protocols for SMC are extension of Shamir's algorithm (1979) and providing us the possibility to calculate the BC preserving the privacy concerns. Furthermore we applied the distributive property of binary operations to calculate the result of Equation (1). This provides us the possibility that private shares of players stay private.

Table 2. Description of the methods of the Player class

Our artifact calculates the values of σ_{st} and $\sigma_{st}(v)$ decentrally. Each players has a part of this information. The methods *calculateNumberOfShortestPaths*() and the *calculatePlayersOnShortestPaths*() calculate each player's σ_{st}^{p} and $\sigma_{st}^{p}(v)$. The final values of σ_{st} and $\sigma_{st}(v)$ are the sum of the decentrally calculated values of all players as follows:

$$\sigma_{st} = \sum_{\forall p \in V} \sigma_{st}^{p}, \qquad \sigma_{st}(v) = \sum_{\forall p \in V} \sigma_{st}^{p}(v) \tag{5}$$

The *calculateSecureBetweenness*() method decentrally calculates the above mentioned sums based on SMC algorithms. In single cases players might infer information when they are called from neighboring players to execute the *calculateNumberOfShortestPaths*() and the *calculatePlayersOnShortestPaths*() methods. Although the players are only able to infer information from their perspective. For instance if the shortest path of a neighboring player to target t is via the current player it implies for the current player that the neighboring player and target t are not neighbors. Whereas it does not contain the information about the forming players of and the number of shortest path(s). Moreover, for privacy preserving concerns players communicate (except the *calculateSecureBetweenness*() method) only via their neighboring players. For this purpose, each object routes its messages through the neighboring players in the network.

Table 3 elaborates sequences of our artifact. Steps 1 to 5 and 9 in Table 3 are not in the focus of this paper and are not influencing our artifact's construction therefore, these steps are not documented in this paper. All methods has been implemented but their respective pseudo code is omitted in this paper. In the following we present a brief illustration of each method.

Step	Executor	Description
		Initialization
1	ISA	Identifies the number of players, n, in the network.
2	ISA	Assigns each participating company a $rowNumber$ (without knowing the real identities of the firms).

Step	Executor	Description
3	ISA	Shares the number of players, n, with all players in the network and notifies the players to initialize a new object.
4	Player	Each player initializes a new object from the Player class and informs ISA.
5	ISA	Notifies all players that the players' objects exit and they are available to execute the methods.
Decentral calculation of the shortest paths and path forming players		
6	Player	Each player executes the *calculateSecureShortestPath*() method for itself as the source player and all given targets in the network.
7	Player	Each player executes the *calculateNumberOfShortestPaths*() method to decentrally set the values of σ_{pt} for each given target t.
8	Player	Each player executes the *calculatePlayersOnShortestPaths*() method to decentrally calculate the values of $\sigma_{pt}(v)$ for itself as the source player and each given target t. By termination of the method for all given targets, the player informs ISA.
Synchronization		
9	ISA	ISA informs every player in the network that the *calculatePlayersOnShortestPaths*() is terminated when it receives the notification of termination from all players. This implies that the variables to calculate the BC are available.
Calculation of the BC		
10	ISA	ISA coordinates players for execution of the *calculateSecureBetweenness*() method. With termination of the method for all players in the network, all firms have their own BCs as well as the BC of all players in the network.

Table 3. The artifact's structure

While we have implemented the described methods, they are not included in this paper.

We represent the *calculateSecureShortestPath*() method with the method's sequence diagram. For reasons of simplicity, Figure 3 provides the *calculateSecureShortestPath*(5,7) from player 5's perspective for our exemplary network (Figure 1). We assumed δ for player 7 is 70.

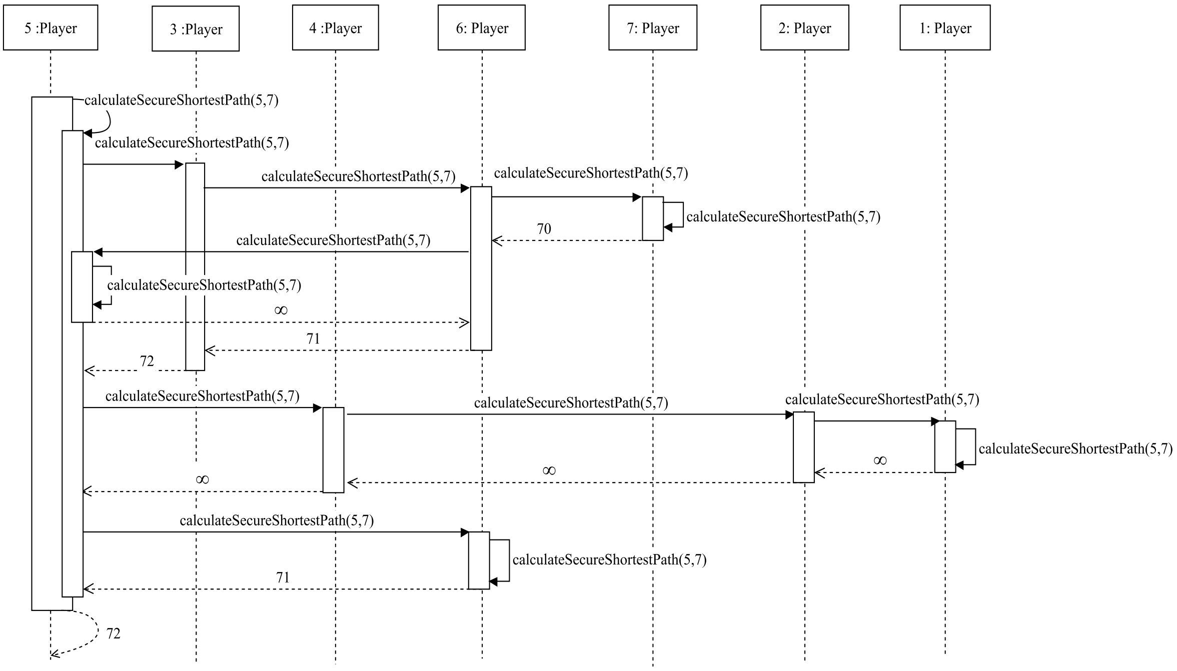

5 :Player
3 :Player
4 :Player
6: Player
7: Player
2: Player
1: Player
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
70
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
∞
71
72
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
∞
∞
∞
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
71
72

Figure 3. Sequence diagram for calculateSecureShortestPath(5,7) from player 5's perspective

The *calculateNumberOfShortestPaths*() method identifies the number of shortest paths from the source player and recursively identifies additional shortest paths via the players who are forming the shortest path(s). For instance player 5 executes the *calculateNumberOfShortestPaths*(5,7) and identifies $\sigma_{57}^{(5)} = 1$. Since player 7 is not a neighboring player of player 5, and player 6 is in Ω_7 player the method calls itself from player 6. Player 6 does not identify any additional path (since player 6's $\Omega_7 = 0$) therefore, it sets $\sigma_{57}^{(6)} = 0$. At this point the method terminates while player 7 (the target) is a neighboring player of player 6.

The *calculatePlayersOnShortestPaths*() method subsequently considers a player on the shortest path(s) between source player s and target player t when the player is in Ω_t of the current player. Moreover it reconsiders the current player (except the case where $s = p$) on the shortest path(s) when current player p has more than one shortest path to the target. For instance the *calculatePlayersOnShortestPaths*(5,7), identifies $\sigma_{57}^{(5)}(6) = 1$ while player 6 is in player 5's Ω_7. Since player 7 is not a neighboring player of player 5, the method calls itself from its neighboring player (player 6). Player 6 is the neighboring player of the target (player 7) therefore, no further calculation takes place and the method terminates.

The *calculateSecureBetweenness*(v) method calculates the BC for player v based on SMC algorithms. In order to facilitate all-to-all communication, ISA coordinates the simultaneous exchange of information. To ensure that the real identities of the firms stay private in an all-to-all communication, existing tools for anonymization can be adapted.

The BC for player v based on Equation (1) is as follows:

$$\mathrm{BC(v)} = \sum_{s \neq v \neq t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}} = \frac{\sigma_{12}(v)}{\sigma_{12}} + \frac{\sigma_{13}(v)}{\sigma_{13}} + \frac{\sigma_{14}(v)}{\sigma_{14}} + \cdots + \frac{\sigma_{ij}(v)}{\sigma_{ij}}, \text{ where } i = |V| \text{ and } j = |V| - 1.$$

For the calculation of the BC we use SMC algorithms. Secure addition and secure multiplication algorithms will, however, reveal a party's input as inverse functions can easily be applied for only two input factors. To keep the input variables in arithmetic operations private, it is necessary that more than two players deliver input. In the above mentioned equation we address this problem. By division of two variables delivered by two players, even with the application of SMC algorithms, the end result reveals the input variables for the players. Therefore, by using a common denominator we solve the problem as follows:

$$\mathrm{BC}(v) = \frac{\sigma_{12}(v) \cdot (\sigma_{12} \cdot \sigma_{13} \cdot \ldots \cdot \sigma_{ij}) + \sigma_{13}(v) \cdot (\sigma_{12} \cdot \sigma_{13} \cdot \ldots \cdot \sigma_{ij}) + \cdots + \sigma_{ij}(v) \cdot (\sigma_{12} \cdot \sigma_{13} \cdot \ldots \cdot \sigma_{ij})}{\sigma_{12} \cdot \sigma_{13} \cdot \sigma_{14} \cdot \ldots \cdot \sigma_{ij}} \tag{6}$$

Furthermore, the values of σ_{st} and $\sigma_{st}(v)$ $\forall s \neq v \neq t \in V$ are the results of Equation (5). For privacy preserving concerns, as addressed in Requirement 1, we do not calculate and share the final values of σ_{st} and $\sigma_{st}(v)$ in the network. Hence, we use the distributive property of arithmetic operations to distributedly consider the components of Equation (5) in Equation (6). Using the mentioned modification on the BC calculation's equation we provide the possibility to keep the private shares of the players private and calculate the BC. The implementation of the artifact with the application of SMC algorithms, anonymization methods, and necessary communication protocols are not covered in this paper.

5 Evaluation

This section provides the evaluation of our artifact. Concerning characteristics of our artifact, we chose the "testing" and "descriptive evaluation" methods based on Hevner et al. (2004) and Gill and Hevner (2013). We implemented a simplified prototype of the artifact. The prototype covers the methods of the class Player. However, the prototype does not cover the implementation of SMC algorithms and assumes they are given. Moreover, the prototype models each player as a local thread, and it is not executed on a distributed system. Furthermore, a third person other than the authors manually evaluated the artifact with a structural walk through the code. In the following we cover general evaluation of completeness, termination, complexity, utility and privacy of the artifact. Furthermore, we illustrate the privacy evaluation based on an application example. Although based on the acceptance and wide application of SMC algorithms we did not analyze their properties. We assume SMC algorithms are complete and secure.

Completeness: To evaluate the artifact in terms of completeness we executed the prototype with various scenarios and evaluated the results. It proved that our approach creates complete results for each given network. Moreover, the structural walk through the code resulted the same.

Termination: By means of testing the prototype in various scenarios as well as structural walk through the code we conducted that the artifact terminates.

Complexity: Analysis of our artifact pointed both the time complexity and the message complexity are polynomial in the maximum distance between the source and the target player, and number of network members. In our artifact we focused to achieve a privacy preserving method. To preserve the privacy, it is necessary for the players to encrypt and exchange data more often compared to some widely used algorithms (e.g. Brandes' algorithm (2001)). Further improvements of computational complexity of the artifact is subject to further research.

Utility: Based on Gregor and Hevner (2013) an artifact evaluation must address the utility of the artifact. Due to the complexity of implementation and evaluation of the artifact's utility in reality, in this paper we evaluated the utility of the artifact based a simplified prototype, and used an application example. Our artifact's characteristics based on Gill and Hevner (2013) are: it is a novel method, which is open because it is possible to modify it, and is interesting because it addresses risk management and sustainability as one of the main concerns of the firms in SCNs.

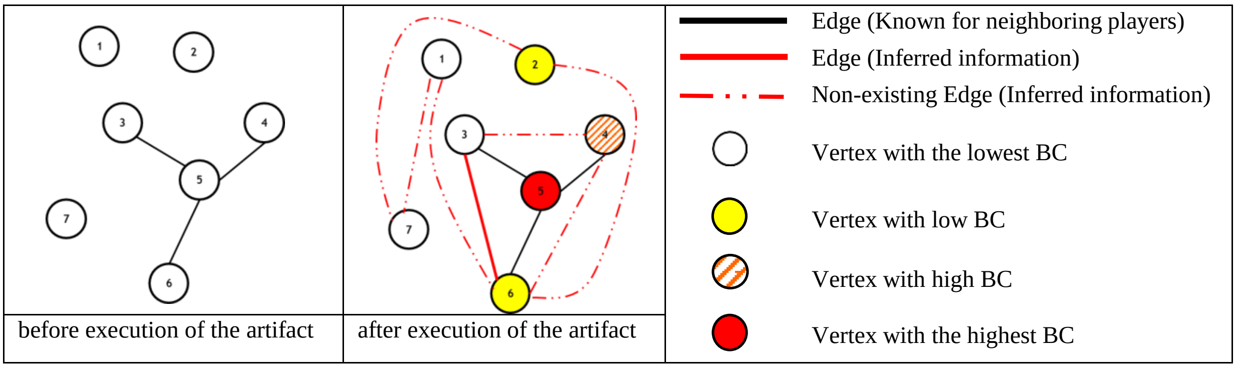
Privacy: The privacy requirements of our artifact (Requirement 1 and 2) are addressed as follows.

- The application of Yao's comparison algorithm and using the modified values for distances ensure that the distances of non-neighboring players stays unknown. Although in a small network, we illustrate in our application example, the distances might be inferable. However, in larger networks (which are in the focus of our research) players cannot infer the distance during the execution of the artifact.
- The number of the shortest paths, and the frequency of appearance of a player on the shortest path are saved decentrally, as mentioned in Equation (5). Therefore, the final values of σ_{st} and $\sigma_{\mathrm{st}}(v)$ are not available to players and stay private.
- By restricting communication via neighboring players and application of anonymization methods, we addressed Requirement 2.

However, we will appreciate if other researchers challenge our artifact in terms of privacy. Furthermore, to illustrate the potential of our artifact to preserve privacy, we describe the artifact's outcome in a short example. Figure 5 provides the network structure from player 5's perspective before and after execution of the method. Based on the result of the BC calculation, players are prioritized and colored as shown in the figure. Player 5 has the highest BC. Player 4 is second. Players 6 and 2 are having the same BC and are standing at the third place. The BC of players 1, 3 and 7 is zero, because they are not on any shortest path. This is a valuable information for all network's members. For instance it implies that if player 5 faces any failure, the whole network's robustness might be at risk. The BC of the players is available for all players in the SCN.

In our exemplary network through execution of the methods, player 5 infers some information. It knows that player 3 and 6 are neighbors, since player 6 and 3 are 5's neighboring players and their shortest paths are not via player 5. Player 5 knows also that players 1 and 6, 2 and 6, as well as 4 and 6 are not neighboring players. The latter information is inferred based on the information that their shortest path is via player 5. But the player is not knowing their exact positioning and if there exists any other alternative shortest path.

It is to conclude that the gained information about the network's structure, even in a small network is limited. By increasing the network's size and complexity the possibility of inferring information decreases. Additionally, the inferred information on non-neighboring vertices is limited. This is similar to a common situation of a SCN. In reality, in a SCN, a company knows more information about its neighbors. The company can partially reveal information about the neighbors of its own neighbors. By going further in the SCN, the company is less capable to deduce the underlying topology or identity of the companies. Moreover, in most of the SCNs, there are some main players that are known by everyone. If other companies identify these firms and their importance, it is not a risk for these players. Their importance and positioning in the network is predictable for most of the firms in the SCN.


1
2
3
4
5
6
7
Edge (Known for neighboring players)
Edge (Inferred information)
Non-existing Edge (Inferred information)
Vertex with the lowest BC
Vertex with low BC
Vertex with high BC
Vertex with the highest BC

before execution of the artifact

after execution of the artifact

Figure 5. The network's structure from player 5's perspective

6 Conclusions

In this paper, we proposed an artifact which preserves privacy and identifies the risky players in the SCNs applying the BC measure. Based on the guidelines of Hevner et al. (2004), and Gregor and Hevner (2013) for conducting design science research, we can summarize our work as follows: Our artifact consists of four main methods. It is an exaptation solution, because we adopted the existing methods in social networks and cryptography algorithms to identify risks in SCNs. Our artifact is formally noted and therefore is well-defined. Based on the literature (e.g. Buhl and Penzel 2010) we addressed two relevant problems: the risk identification in SCNs and privacy concerns of firms in SCNs. We focused on the study of Kim et al. (2011) and decided to calculate the BC as a measure to identify risky firms. In the evaluation section, beside the testing and descriptive evaluation, we illustrated that in our artifact, even in a small exemplary network, the inferred information is limited. To develop a rigorous artifact, we applied well established methods of other fields and extended them to our problem context. Regarding the communication of our result, we choose the evolving technical solutions in computer science and network theory, to answer the question of risk management in SCNs.

In this paper, we focused on identifying risks and kept the information as private as possible. However, higher visibility in the network facilitates improved risk management (Basole and Bellamy 2014). Therefore, it might be necessary that companies agree on sharing more information than the BCs. For instance they might decide to reveal the identities of companies with the BC among top 10%, because they are the most risky ones for the network. On the one hand the more information is shared, the highest is the privacy at risk, and on the other hand it is inevitable to share extra information to reach the network's robustness. Hence, the companies in the network should deal with the trade-off between sharing additional information to facilitate risk management in the network or preserve their privacy.

Although the BC measure identifies the risks in the SCN, integration of complementary network analysis methods (e.g. Newman 2010) in our artifact for an enhanced risk identification, is subject to further research. It is also important to study the intensity of connection and their impacts on the network. These subjects as well as improvement of computational complexity are subject to further research.

References

Abbe, E.A., A.E. Khandani and A.W. Lo (2012). "Privacy-preserving Methods for Sharing Financial Risk Exposures." *The American Economic Review* 102 (3), 65-70.

Arns, M., M. Fischer, P. Kemper and C. Tepper (2002). "Supply Chain Modelling and Its Analytical Evaluation." *Journal of the Operational Research Society* 53 (8), 885-894.

Babich, V., A.N. Burnetas and P.H. Ritchken (2007). "Competition and diversification effects in supply chains with supplier default risk." *Manufacturing & Service Operations Management* 9 (2), 123-146.

Basole, R.C. and M.A. Bellamy (2014). "Supply Network Structure, Visibility, and Risk Diffusion: A Computational Approach." *Decision Sciences* 45 (4), 753-789.

Beaver, D., S. Micali and P. Rogaway (1990). "The Round Complexity of Secure Protocols." In: *Proceedings of the twenty-second annual ACM symposium on Theory of computing.* Ed. by H. Ortiz. Baltimore, MD, USA, 503-513.

Bellamy, M.A. and R.C. Basole (2013). "Network Analysis of Supply Chain Systems: A Systematic Review and Future Research." *Systems Engineering* 16 (2), 235-249.

Blackhurst, J., T. Wu and P. O'grady (2004). "Network-based Approach to Modelling Uncertainty in a Supply Chain." *International Journal of Production Research* 42 (8), 1639-1658.

Blome, C. and T. Schoenherr (2011). "Supply chain risk management in financial crises—A multiple case-study approach." *International Journal of Production Economics* 134 (1), 43-57.

Bogetoft, P., I. Damgård, T. Jakobsen, K. Nielsen, J. Pagter and T. Toft (2006). "A Practical Implementation of Secure Auctions Based on Multiparty Integer Computation." *Financial Cryptography and Data Security* 4107, 142-147.

Booch, G. (1993). *Object-oriented analysis and design with applications.* Addison-Wesley.

Brandes, U. (2001). "A faster algorithm for betweenness centrality*." *Journal of Mathematical Sociology* 25 (2), 163-177.

Brickell, J. and V. Shmatikov (2005). "Privacy-preserving graph algorithms in the semi-honest model." *Advances in Cryptology-ASIACRYPT 2005*, 236-252.

Buhl, H.U. and H. Penzel (2010). "The Chance and Risk of Global Interdependent Networks." *Business & Information Systems Engineering* 2 (6), 333-336.

Canetti, R. (2008). "Theory of cryptography." In: *Proceedings of the fifth theory of cryptography conference, TCC.* Ed. by R. Canetti. New York, USA.

Choi, T.Y. and D.R. Krause (2006). "The supply base and its complexity: implications for transaction costs, risks, responsiveness, and innovation." *Journal of Operations Management* 24 (5), 637-652.

Choi, T.Y. and Y. Hong (2002). "Unveiling the structure of supply networks: case studies in Honda, Acura, and DaimlerChrysler." *Journal of Operations Management* 20 (5), 469-493.

Chu, L.K., Y. Shi, S. Lin, D. Sculli and J. Ni (2010). "Fuzzy chance-constrained programming model for a multi-echelon reverse logistics network for household appliances." *Journal of the Operational Research Society* 61 (4), 551-560.

Cormen, T.H., C.E. Leiserson, R.L. Rivest and C. Stein (2001). *Introduction to algorithms.* MIT press Cambridge.

Cramer, R., I. Damgard and J.B. Nielsen (2013). *Secure Multiparty Computation and Secret Sharing: An Information Theoretic Approach.* Aarhus Unoversity, Denmark: Aarhus University.

Dijkstra, E.W. (1959). "A note on two problems in connexion with graphs." *Numerische mathematik* 1 (1), 269-271.

Dolev, D. and A. Yao (1983). "On the security of public key protocols." *Information Theory, IEEE Transactions on* 29 (2), 198-208.

Edmonds, N., T. Hoefler and A. Lumsdaine (2010). "A space-efficient parallel algorithm for computing betweenness centrality in distributed memory." In: *Proceedings of the International Conference on High Performance Computing (HiPC).* Goa, India, 1-10.

Emmerson, C., V. Ivarsson, J. Lanitis et al. (2008). *Global Risk 2008.*

Floyd, R.W. (1962). "Algorithm 97: shortest path." *Communications of the ACM* 5 (6), 345.

Freeman, L.C. (1977). "A set of measures of centrality based on betweenness." *Sociometry*, 35-41.

Fridgen, G., C. Stepanek and T. Wolf (2014). "Investigation of exogenous shocks in complex supply networks–a modular Petri Net approach." *International Journal of Production Research* (ahead-of-print), 1-22.

Giannakis, M. and M. Louis (2011). "A multi-agent based framework for supply chain risk management." *Journal of Purchasing and Supply Management* 17 (1), 23-31.

Gill, T.G. and A.R. Hevner (2013). "A fitness-utility model for design science research." *ACM Transactions on Management Information Systems (TMIS)* 4 (2), 5.

Goldreich, O., S. Micali and A. Wigderson (1987). "How to Play any Mental Game - A Completeness Theorem for Protocols with Honest Majority." In: *Proceedings of the nineteenth annual ACM Symposium on the Theory of Computing.* Ed. by A.V. Aho. New York, NY, USA, 218-229.

Gregor, S. and A.R. Hevner (2013). "POSITIONING AND PRESENTING DESIGN SCIENCE RESEARCH FOR MAXIMUM IMPACT." *MIS Quarterly* 37 (2), 337-A-6.

Gyorey, T., M. Jochim and S. Norton (2011). "The challenges ahead for supply chains." *McKinsey on Supply Chain: Select Publications*, 10-15.

Hallikas, J., I. Karvonen, U. Pulkkinen, V.M. Virolainen and M. Tuominen (2004). "Risk management processes in supplier networks." *International Journal of Production Economics* 90 (1), 47-58.

HBR Advisory Council (2010). "Is Your Supply Chain Sustainable?" *Harvard Business Review;* 88 (10), 74-74.

Hevner, A.R., S.T. March, J. Park and S. Ram (2004). "Design science in information systems research." *MIS quarterly* 28 (1), 75-105.

Hochberg, Y.V., A. Ljungqvist and Y. Lu (2007). "Whom you know matters: Venture capital networks and investment performance." *The Journal of Finance* 62 (1), 251-301.

Huang, Y., J. Katz and D. Evans (2012). "Quid-pro-quo-tocols: Strengthening semi-honest protocols with dual execution." In: *Proceedings of the Security and Privacy (SP), 2012 IEEE Symposium on.* San Francisco, California, USA, 272-284.

Jacob, R., D. Koschützki, K.A. Lehmann, L. Peeters and D. Tenfelde-Podehl (2005). "Algorithms for centrality indices." *Network Analysis.* Springer, Berlin Heidelberg.

Kerschbaum, F. (2011). "Secure and sustainable benchmarking in clouds." *Business & Information Systems Engineering* 3 (3), 135-143.

Kerschbaum, F., A. Schröpfer, A. Zilli et al. (2011). "Secure Collaborative Supply-Chain Management." *Computer* 44 (9), 38-43.

Kersten, W., P. Hohrath and M. Winter (2008). "Risikomanagement in Wertschöpfungsnetzwerken–Status quo und aktuelle Herausforderungen." *Supply Chain Risk Management*, 7.

Kim, Y., T.Y. Choi, T. Yan and K. Dooley (2011). "Structural investigation of supply networks: A social network analysis approach." *Journal of Operations Management* 29 (3), 194-211.

Klein, D. (2010). "Centrality measure in graphs." *Journal of mathematical chemistry* 47 (4), 1209-1223.

Lessard, D.R. (2013). "Uncertainty and Risk in Global Supply Chains." *MIT Sloan Research Paper No. 4991-13.*

Li, M. and T.Y. Choi (2009). "Triads in Services Outsourcing: Bridge, Bridge Decay and Bridge Transfer*." *Journal of Supply Chain Management* 45 (3), 27-39.

Lindell, Y. and B. Pinkas (2009). "A proof of security of Yao's protocol for two-party computation." *Journal of Cryptology* 22 (2), 161-188.

Mizgier, K.J., M.P. Jüttner and S.M. Wagner (2013). "Bottleneck identification in supply chain networks." *International Journal of Production Research* 51 (5), 1477-1490.

Moore, E.F. (1959). "The shortest path through a maze." In: *Proceedings of the Proceedings of the International Symposium on the Theory of Switching.* Ed. by Harvard University Press. , 285-292.

Newman, M. (2010). *Networks: an introduction.* Oxford University Press, Inc.

Peck, H. (2003). *Creating Resilient Supply Chains: A Practical Guide.* United Kingdom: Cranfield University.

Reistad, T.I. (2012). "Multi-party secure position determination." *A General Framework for Multiparty Computations.* Norwegian University of Science and Technology, Trondheim.

Russell, S. and P. Norvig (2009). *Artificial Intelligence: A Modern Approach.* Prentice Hall.

Schneider, T. (2012). *Engineering Secure Two-Party Computation Protocols.* Springer.

Shamir, A. (1979). "How to share a secret." *Communications of the ACM* 22 (11), 612-613.

Sheikh, R., B. Kumar and D.K. Mishra (2009). "Privacy Preserving k Secure Sum Protocol." *International Journal of Computer Science and Information Security* 6 (2), 184-188.

Venable, J., J. Pries-Heje and R. Baskerville (2012). "A comprehensive framework for evaluation in design science research." *Design Science Research in Information Systems. Advances in Theory and Practice.* Springer, Berlin Heidelberg.

Vereecke, A., R. Van Dierdonck and A. De Meyer (2006). "A typology of plants in global manufacturing networks." *Management Science* 52 (11), 1737-1750.

Wagner, S.M. and N. Neshat (2012). "A comparison of supply chain vulnerability indices for different categories of firms." *International Journal of Production Research* 50 (11), 2877-2891.

Warshall, S. (1962). "A theorem on boolean matrices." *Journal of the ACM (JACM)* 9 (1), 11-12.

Wasserman, S. and K. Faust (1994). *Social network analysis: Methods and applications.* Cambridge university press.

Yao, A.C. (1986). "How to generate and exchange secrets." In: *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*, 162-167.

Yao, A.C. (1982). "Protocols for secure computations." In: *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, 160-164.

Yates, J.F. and E.R. Stone (1992). "The risk construct." *Risk-taking Behavior.* John Wiley & Sons, New York.

Zhao, K., A. Kumar, T.P. Harrison and J. Yen (2011). "Analyzing the resilience of complex supply network topologies against random and targeted disruptions." *Systems Journal, IEEE* 5 (1), 28-39.