IET Research Journals

Submission Template for IET Research Journal Papers

Journals
The Institution of
Engineering and Technology

Fair and Private Rewarding in a Coalitional Game of Cybersecurity Information Sharing

ISSN 1751-8644
doi: 0000000000
www.ietdl.org

Iman Vakilinia[1*], *Shamik Sengupta*[1]

[1] *Department of Computer Science and Engineering, University of Nevada Reno, 1664 N. Virginia Street, Reno 89557, USA*
* *E-mail: ivakilinia@unr.edu*

Abstract: Cybersecurity information sharing is a key factor of cyber threat intelligence, allowing organizations to detect and prevent malicious behaviors proactively. However, stimulating organizations to participate and deterring free-riding in such sharing is a big challenge. To this end, the sharing system should be equipped with a rewarding and participation-fees allocation mechanisms to encourage sharing behavior. The problem of cybersecurity information sharing as a non-cooperative game has been studied extensively. In contrast, in this paper, we model such a problem as a coalitional game. We investigate a rewarding and participation-fees calculation based on profit sharing in coalitional game theory. In particular, we formulate a coalitional game between organizations and analyze the well-known *Shapley value* and *Nucleolus* solution concepts in the cybersecurity information sharing system. Moreover, as the participation-fees may leak sensitive information about the organizations' cyber-infrastructure, we study the application of differential privacy in the coalitional game theory to protect the organization's fees while approximating the fairness.

1 Introduction

The frequency and complexity of cyber-attacks have increased with the significant growth of our daily life dependency to the cyberspace. To get ahead of the security threats, it is crucial to have a proactive security approach to prevent any dangers before they occur. Cybersecurity information sharing is a key factor in proactively defending against sophisticated cyber-attacks [1]. Moreover, such sharing decreases the time and enhances the accuracy of the detection and prevention of malicious behaviors in the system. Due to the importance of cybersecurity information sharing, governmental laws/initiatives have been legislated to mandate/encourage the governmental and private organizations to share their cybersecurity information [2]. For instance, the US Senate has passed the Cybersecurity Information Sharing Act (CISA) [3] federal law designed to improve cybersecurity through enhanced sharing of information about cybersecurity threats. The law allows the sharing of Internet traffic information between the US government and private companies. In the UK, Cybersecurity Information Sharing Partnership (CiSP) [4] is an initiative for industry and government that has been set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment to increase situational awareness and reduce the impact on UK business. EU has also launched several cross-sector and intra-sector initiatives to enhance the EU Member States capability for preparedness, cooperation, information exchange, coordination, and response to cyber threats [5].

In the private sector, the organizations act as self-interested rational players and sharing cybersecurity information can be costly for the information possessor. For example, attackers might utilize the shared information for reconnaissance, the competitive organization might take advantage of the shared information which indirectly affects the organization's utility, and sensitive private information (such as names and email addresses) might leak out. On the other hand, the finder of a vulnerability can sell it on the black market. Thus, stimulating the owner of cybersecurity information to choose sharing behavior is a big challenge.

Recently, plenty of research has been done in modeling the benefit and cost of the cybersecurity information sharing by applying game theory [6–8]. Traditionally the cybersecurity information sharing is modeled as a non-cooperative game where the players are the organizations, and the strategies are choosing between sharing and not-sharing. In this case, we have the following conditions: if none of the organizations share their information, the organizations' payoffs are zero, if some of the organizations participate in sharing, but the others refuse to reciprocate, then the organizations who refused, receive better payoff than the rest of them. Finally, if all of the organizations share, then all of them benefit from sharing. This game resembles the well-known Prisoner's Dilemma game [9]. Although the best payoff is received from mutual sharing, players choose not-sharing as their Nash Equilibrium approach.

To change the equilibrium point to the sharing strategy, we need a mechanism to stimulate the sharing behavior. Here, choosing the proper rewarding value is a big challenge. To stimulate organizations to share applicable information, the reward should be an increasing function of the total benefits of the other organizations applying the information. Furthermore, as we assume the organizations are the only financial sources of the cybersecurity information sharing system, the total rewards are equal to the total amount of organizations' participation-fee. The participation-fee calculation ought to prevent organizations from free-ride by taking advantage of shared information without participation. Furthermore, this fee should be fair, such that the organizations' payment should be proportional to their benefits from the information.

On the other hand, organizations' participation-fees are classified as confidential information since they reveal the organizations' cyber-infrastructure configuration through the organizations' cybersecurity investment tendency [10]. Disclosure of organizations' participation-fee, paves the attackers' way for reconnaissance to exploit the organizations' vulnerabilities. Thus, the value of organizations' participation-fee should be protected. As an example, consider that a vulnerability in a specific database management system has been detected and an organization is interested to pay a big amount of money to access such information. Such an investment tendency allows an attacker to have a better picture of the target's cyber-infrastructure configuration.

In this paper, we investigate the fair and private rewarding and participation-fee calculation by applying the coalitional game theory and differential privacy in the cybersecurity information sharing system. The main objective of our proposed mechanism is to stimulate organizations to share more useful information with the goal of increasing the organizations' payoff fairly while preserving the participants' participation-fee private. To achieve this goal, first we investigate the solution concepts of *Shapley value* and *Nucleolus* allocations in the cybersecurity information sharing game. Second, we inspect the differential privacy concept in the coalitional cybersecurity information sharing rewarding.

The main contributions of this paper are the two parts, as described below:
1- We present a novel coalitional game for rewarding and participation-fee allocation in the cybersecurity information sharing, and then we investigate the *Shapley value* and *Nucleolus* distribution solution concepts of utility among organizations in the cybersecurity information sharing.
2- We investigate the application of differential privacy in coalitional game theory. For this purpose, we relax the fairness definition by introducing δ-fair concept. Then, we study the rewarding mechanism in the coalitional cybersecurity information sharing environment, such that the organizations' participation-fees are protected from an adversary with side information.

To the best of our knowledge, this research is the first work to investigate the fair and differentially private rewarding and participation-fee allocation in the cybersecurity information sharing. Our mechanism can also be applicable to other profit sharing settings as well.

A preliminary version of this work appeared in [11], where we modeled a cybersecurity information sharing platform as a cooperative game and we investigated the *Shapley value* and *Nucleolus* distribution solution concepts. We extend our previous work by proposing a new privacy-preserving model for profit sharing considering the fairness requirement. For this purpose, we have applied the differential privacy concept.

The rest of the paper is structured as follows. Next section reviews major related works in the cybersecurity information sharing, coalitional game, and differential privacy. In section 3, we state the problem. We investigate the coalitional formation in the cybersecurity information sharing environment in section 4. Section 5 presents our differentially private and fair profit sharing in the cybersecurity information sharing coalitional game. Simulation result is presented in section 6. We conclude our paper in section 7.

2 Related Works

2.1 Cybersecurity Information Sharing

Cybersecurity information sharing and risk interdependency have been studied extensively in [12–20]. Rutkowski et al. [12] have investigated the specification and use case of the cybersecurity information exchange framework. To facilitate sharing the cybersecurity information, various protocols and standards have been proposed such as TAXII, STIX, and CybOX [14, 15]. The cybersecurity information sharing in competitive environments with the game theory approach has been studied in [7, 8]. Economic analysis of cybersecurity information sharing and applying incentives for motivation have been studied in [6].

On the other hand, the role of a social planner to control free-riding in cybersecurity information sharing game has been investigated in [19]. Mandatory security breach reporting through security audits and imposing sanctions have been studied in [13].

Privacy risks in sharing cybersecurity information have been studied in [21]. In this work, the authors have studied the trade-off between the need for potentially sensitive data, and the perceived privacy risk of sharing that data.

In [22], Garrido-Pelaz et al. analyze the benefits and drawbacks of information sharing by proposing a model among organizations with the different level of dependency. The proposed model applies functional dependency network analysis to investigate the attacks propagation and game theory for information sharing management.

Tosh et al. [23] present a game theoretic framework to investigate the economic benefits of cyber-threat information sharing and analyze the impacts and consequences of not participating in the game of information exchange. They model the information exchange framework as distributed non-cooperative game among the firms and investigate the implications of information sharing and security investments.

In [24], Tosh et al. have investigated the cybersecurity information sharing from an evolutionary game theoretic strategy and investigated the conditions under which the players' self-enforced evolutionary stability can be achieved. Furthermore, the authors have presented a heuristic approach to obtain an evolutionary stable strategy.

We have also studied the security and privacy issues of cybersecurity information sharing and proposed different mechanisms to overcome such challenges in our previous works [17, 25, 26]. A framework for privacy preservation of cybersecurity information sharing has been proposed in [26]. This scheme uses group signature to hide the identities of the organizations. However, this scheme does not protect the participants' information.Vakilinia et al. [25] have modeled the privacy issue in cybersecurity information sharing as a game between organizations and attackers. Although such a model helps the organizations to decide their sharing strategy, it does not provide any practical solution to protect the underlying information.

However, in contrast to previous works, we model the cybersecurity information sharing as a cooperative game in this work, then, we analyze the rewarding and participation-fee allocation according to the organization's benefits obtained from the sharing platform. We investigate the solution concepts for fair and differentially private allocation of utility among the players.

Note that, although the problem of cybersecurity information sharing has similarities to the problem of secret sharing, they are not equal. The secret sharing is a well-known cryptographic primitive that allows an entity to share a secret among n other agents, so that any m of them may reconstruct it. The logic behind this protocol is that, of the n agents, at most $(n - m)$ are "bad". While the bad agents might not cooperate, the good agents will follow the protocol and pool their share of the secret [27]. However, in the cybersecurity information sharing, there is no bad agent among organizations who want to access the information, on the other hand, the information owner is not willing to share its information unless it gets a reward from the sharing platform. In this scenario, there is no subset of n to open the information, and the information owner decides to share its data if the reward is satisfying. In the paper, we have modeled a cooperative game between organizations to study the fair profit sharing in cybersecurity information sharing platform. In this work, we are interested to analyze the fair profit sharing in a cooperative game setting.

It is also worth to mention that Goldman and Zilberstein [28] have studied the problem of information exchange in the multi-agent systems where the problem is to decide the optimal rate of information exchange among agents considering the cost of sharing information with the risk of revealing it to competing agents in an unreliable connection.

2.2 Privacy Preserving Methods

As in the cybersecurity information sharing, rewarding and participation-fee leaks sensitive information about the organizations' cyber-infrastructure [10], we aim to protect those values. Applying cryptographic techniques, many research studies have been done to protect the private information while allowing the computation of a function. For instance, secure multiparty computation [29] and homomorphic encryption [30] are introduced to compute the result of a function without revealing the sensitive input parameters belonging to the entities. Despite the benefit of such methods, an attacker with side information accessing the output value can still infer private information. In order to overcome this challenge, perturbation techniques have been introduced [31]. In such methods, the output is perturbed to preserve the individual values private in the result while keeping the output utility as much as possible.

Differential privacy [32] is a well-known provable concept in the privacy literature which is independent of adversary and data. Differential privacy was first proposed to protect the statistical database where a trusted curator perturbs responses for the queries. Afterwards, this concept has been more developed in many other studies such as data-mining [33], mechanism design [34, 35], smart metering [36, 37], and distributed stream monitoring [38].

Table 1 Feature Set of Vulnerability CVE-2016-10012 (http://www.cvedetails.com/cve/CVE-2016-10012/)

Feature	***Description***
CVSS	7.2
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Overflow Gain privileges
CWE ID	119
Vendor, Product, Version	Openbsd, Openssh, 7.3

In this paper, we investigate differentially private profit sharing in the coalitional game setting. Specifically, we apply differential privacy to preserve the privacy of the participation-fee in the cybersecurity information sharing. To the best of our knowledge, this work is the first research to investigate the differential privacy in the fair profit sharing of the coalitional game theory.

3 Overview and Problem Statement

Let $O = \{o_1, ..., o_n\}$ represent the organizations participating in cybersecurity information sharing. Although various information can be shared among organizations such as raw network logs, attackers techniques, the signature of attacks, and the vulnerabilities' details, in this work, we particularly focus on sharing discovered security vulnerabilities as in [8]. In each sharing cycle, a set of vulnerabilities $V = \{v_1, ..., v_m\}$ will be detected by the participant organizations. For example, a cycle can be a time window of a year. Each vulnerability is associated with a unique feature set $F_{v_k \in V}$, which is the vulnerability specification.

As an example, consider vulnerability CVE-2016-10012. The feature set of this vulnerability is shown in Table 1. In this table, CVSS (Common Vulnerability Scoring System, https://nvd.nist.gov/vuln-metrics/cvss) is a metric for the calculation of vulnerabilities' impacts, and CWE (Common Weakness Enumeration, https://cwe.mitre.org/) represents the weakness category.

Having F_{v_k}, organizations can calculate the expected cost of vulnerability exploitation. For example, assume there is a vulnerability allowing the attackers to gain access to the data of a database system. This can be realized from the vulnerability properties CVE. The exposing of underlying data has different costs for the organizations. Therefore, the organizations would value the vulnerability information differently considering the cost and benefit of patching their vulnerable systems. Such valuations are performed considering the risk estimation of the exploitation of the vulnerabilities associated with the affected assets. Let $\pi_i(F_{v_k})$ be the expected cost of exploitation of vulnerability v_k for o_i. Let $\mathcal{P}_i(F_{v_k})$ and $\mathcal{E}_i(F_{v_k})$ denote the probability and the cost of successful exploitation of v_k for o_i, respectively. Thus, we can calculate the expected cost as

$$\pi_i(F_{v_k}) = \mathcal{P}_i(F_{v_k}) \times \mathcal{E}_i(F_{v_k}) \tag{1}$$

In the rest of paper, we will denote $\pi_i(F_{v_k})$ with $\pi_{i,k}$ for simplicity. If o_i patches the vulnerability by accessing the shared information before exploitation, then $\pi_{i,k}$ is the expected benefit of accessing the shared information for o_i regarding the vulnerability v_k.

We assume there is a trusted third party server $\mathcal{S}$, verifying the vulnerability information and computing the participation-fee and reward for the players.

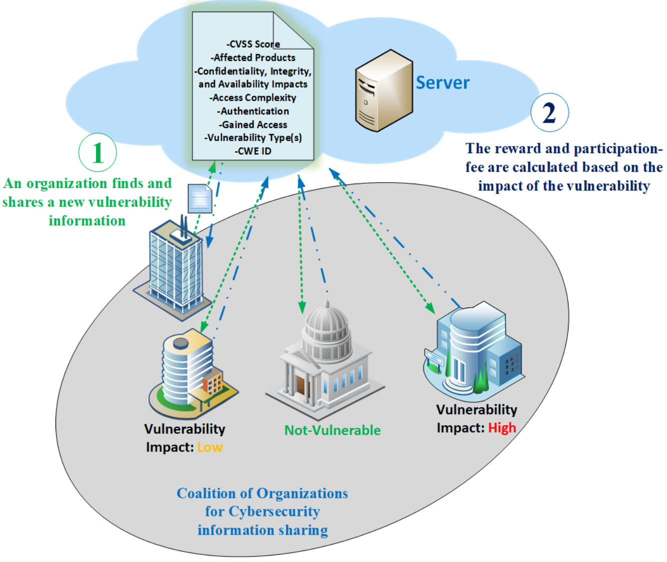
Once o_j submits the vulnerability information v_k to $\mathcal{S}$, $\mathcal{S}$ first verifies it and then calculate the reward $r_{j,k}$. The reward $r_{j,k}$ is the total payment of the other participant organizations $o_{i \neq j}$ for accessing the vulnerability information v_k. Let $x_{i,k}$ denote the o_i's payment for accessing the shared information of the vulnerability v_k. Hereafter, the term *participation-fee* represents $x_{i,k}$. The possessor of vulnerability information decides whether to share the vulnerability information or not, based upon the proposed reward value $r_{j,k} = \sum_{o_i \in O} x_{i,k}$. Let f_i denote the membership-fee of o_i at the end of cybersecurity information sharing, then f_i is computed as

$$f_i = \sum_{v_k \in V} (x_{i,k} - r_{i,k}) \tag{2}$$

The steps of information sharing are as follows. At the first step, organizations register into the system by providing the certificates and their platform information to $\mathcal{S}$. As the vulnerability information is sensitive and can be used by malicious entities to attack the other systems, in the proposed model, the framework requires to authenticate the organizations to prevent the entrance of malicious entities. When a new vulnerability has been detected by one of the members, $\mathcal{S}$ calculates the patching benefit and participation-fee for the organizations getting advantage of such information. Then, based on the total participation-fee, $\mathcal{S}$ computes the reward value for the information possessor.

When a cybersecurity information sharing cycle ends, $\mathcal{S}$ calculates the membership-fee f_i. If f_i is negative, then $\mathcal{S}$ pays corresponding amount to o_i, and if f_i is positive, then o_i pays corresponding amount to $\mathcal{S}$.

Figure 1 displays the general architecture of cybersecurity information sharing system, and Figure 2 depicts the overall picture of participation-fee and reward calculation.



-CVSS Score
-Affected Products
-Confidentiality, Integrity, and Availability Impacts
-Access Complexity
-Authentication
-Gained Access
-Vulnerability Type(s)
-CWE ID
Server
1
An organization finds and shares a new vulnerability information
2
The reward and participation-fee are calculated based on the impact of the vulnerability
Vulnerability Impact: Low
Not-Vulnerable
Vulnerability Impact: High
Coalition of Organizations for Cybersecurity information sharing

Fig. 1: The cybersecurity information sharing platform

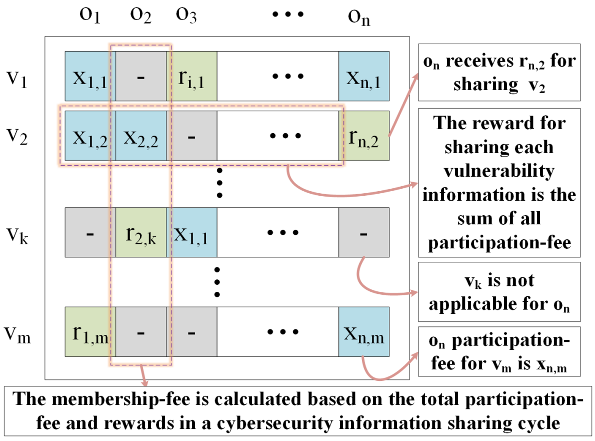

o1 o2 o3 ••• on
v1 x1,1 - ri,1 ••• xn,1
v2 x1,2 x2,2 - ••• rn,2
vk - r2,k x1,1 ••• -
vm r1,m - - ••• xn,m
on receives rn,2 for sharing v2
The reward for sharing each vulnerability information is the sum of all participation-fee
vk is not applicable for on
on participation-fee for vm is xn,m
The membership-fee is calculated based on the total participation-fee and rewards in a cybersecurity information sharing cycle

Fig. 2: The calculation of reward and participation-fee

On the other hand, we assume there is an adversary accessing the reward value $r_{i,k}$, and aiming to estimate the victim organization's participation-fee. We assume adversary has side information and organizations might collude with an adversary by sharing their participation-fee. In this case, an adversary is interested in finding the organization's participation-fee to gain information about the IT infrastructure of the victim. For example, if an adversary knows that the victim is willing to pay a large value for a vulnerability of specific database management system, it can conclude that the victim is using such a database management system to store valuable information. It is also worth to mention that, the proposed mechanisms are not limited to profit sharing in cybersecurity information sharing, but can also be applied to other profit sharing schemes which expect private profit allocation. Our goal is to present an efficient mechanism for preserving the privacy of an organization's participation-fee while approximating fair profit sharing in the process of rewarding. More specifically, the fair and private mechanism should satisfy the following requirements.

Fairness The rewarding and participation-fee allocation should be fair, such that the reward is calculated based on the organizations' advantage from the information, and participation-fee is calculated based on the advantage receives from the information. Furthermore, in the privacy preserving model, the cost of augmented noise to the reward value should be distributed fairly among participants.

Privacy The mechanism should prevent an adversary with side information to infer an organization's participation-fee. An adversary might have access to participation-fees of some organizations by colluding with them.

Having this system model, first we study the fair profit sharing among organizations by investigating the *Shapley value* and *Nucleolus* solution concepts. Then, we examine the private rewarding method to protect an organization's participation-fee $x_{j,k}$ from an adversary with the side information. To achieve this goal, we present a differentially private rewarding mechanism.

4 Rewarding in Coalitional Game with Transferable Utility

In this section, first, we introduce the coalitional games, then we investigate the requirements of participation-fee and reward calculation for cybersecurity information sharing system. Finally, we analyze the solution concepts for the coalitional formation of cybersecurity information sharing game.

4.1 Coalitional Game

Coalitional game theory studies the behavior of rational self-interested players in strategic settings where players reach agreements to elevate their payoffs. The main question in a coalitional game is how to share the benefits among agents in a coalition. The most well-known solution concepts for such sharing are the *Shapley value* [39] and the *Nucleolus* [40]. Saad et al. [41] classify the coalitional game into three different groups as canonical coalitional games, coalition formation games, and coalitional graph games. In canonical coalitional games, the problem is to stabilize the grand coalition. The grand coalition of all users is an optimal structure. In coalition formation games, the network structure that forms depends on gains and costs from cooperation and the problem is how to form an appropriate coalitional topology. In coalitional graph games, players' interactions are governed by a communication graph structure and the problem is to stabilize the grand coalition or form a network structure taking into account the communication graph.

Since in cybersecurity information sharing system, the goal is to have the grand coalition of the entities to maximize the benefits of sharing information, the problem of proper rewarding and participation-fee allocation falls into canonical coalitional games category. Canonical coalitional games have been studied in the wireless network area. For instance, Singh et al. [42] discuss the profit sharing in coalition base resource allocation in wireless networks, and fair payoff allocation for cooperation in wireless ad-hoc networks using *Shapley value* is studied in [43]. Muto et al. [44] categorize a set of coalitional games as *big-boss* games. In such games, the coalition value is dependent on the existence of a specific player (namely *big-boss*) in the coalition. The coalition of subsets not containing the *big-boss* receives zero value. In this work, we model the cybersecurity information sharing as a coalitional game such that if the information possessor does not locate in the coalition then there is no benefit for any member of the coalition. Hence, this game is a subset of *big-boss* games. Afterward, we investigate the solution concepts of profit sharing in the cybersecurity information sharing game.

As pointed out earlier, typically organizations are not willing to share their cybersecurity information because of the sharing cost. Let $\tau_{i,k}$ denote the sharing cost of v_k for o_i, then o_i would share v_k if and only if $\tau_{i,k} < r_{i,k}$. Besides that, the impacts of vulnerabilities are not equal and other organizations $o_{j \neq i}$, would pay $x_{j,k}$ to access v_k to patch their systems as long as the patching benefit outweighs the participation-fee, in other words we have $x_{j,k} < \pi_{j,k}$. If $x_{j,k}$ is small, then the reward may not be motivative for o_i, and as a result, o_i will not share the information, resulting in risk of vulnerability exploitation for o_j. On the other hand, if $x_{j,k}$ is large, then the margin of profit for o_j is small. Thus, in this setting, we are interested in the fair distribution of the utilities among organizations to satisfy all of them. To achieve this goal, first, we define the following features for the rewarding mechanism in cybersecurity information sharing.

Definition 4.1. The rewarding mechanism of the cybersecurity information sharing is *dynamic* if it calculates the reward based on the overall benefits to the system. In the dynamic rewarding mechanism, the participants are motivated to share more useful information since the reward is an increasing function of the benefits achieved by the other organizations exploiting the shared information.

Definition 4.2. The rewarding mechanism of the cybersecurity information sharing is *fair* if the participation-fee for beneficiary organizations is calculated based on their advantages from accessing the information. If the rewarding mechanism is not fair, organizations may not contribute to the reward value (since their benefits may not outweigh the payment cost). In this case, the reward may not be motivative for the information possessor and as a result, the information will not be shared in the system.

Definition 4.3. The rewarding mechanism of the cybersecurity information sharing is *stable*, if it is dynamic and fair.

As we are interested in finding the *stable* rewarding mechanism, we investigate the profit sharing in the coalition formation of cybersecurity information sharing.

4.2 Profit Sharing

In coalitional game with transferable utility, an n-person game is given by the pair $G(N, \mathrm{v})$, where $N = \{1, 2, ..., n\}$ is the set of players and v is a real-valued payoff that the coalition's members can distribute among themselves. v is also called the characteristic function of the game, which returns a value for each subset of N. In other words $\mathrm{v} : 2^N \rightarrow \mathbb{R}$. *Superadditivity* and *Convexity* of the game are defined as follows.

Definition 4.4. (*Superadditivity*) A game $G(N, \mathrm{v})$ is superadditive, if for all $S, T \subset N$ and $(S \cap T = \emptyset)$, then $\mathrm{v}(S) + \mathrm{v}(T) \leq \mathrm{v}(S \cup T)$.

Definition 4.5. (*Convexity*) A game $G(N, \mathrm{v})$ is convex if for all $S, T \subset N$, then $\mathrm{v}(S \cup T) \geq \mathrm{v}(S) + \mathrm{v}(T) - \mathrm{v}(S \cap T)$.

While the characteristic function describes the payoff available to coalitions, it does not prescribe a way of distributing these payoffs. An allocation is a vector $\bar{x} = (x_1, ..., x_n)$ assigning payoff to each player. In the cybersecurity information sharing game, we are looking for an allocation which stimulates organizations to make the largest coalition. In other words, we are looking for an allocation which is located in the *Core*.

Definition 4.6. (*Core*) An allocation x is in the core of $G(N, \mathrm{v})$ iff $x(N) = \mathrm{v}(N)$ and for any $S \subseteq N$ we have $x(S) \geq \mathrm{v}(S)$. In words, core is the set of x payoff allocations with the property that no coalition of agents can guarantee all of its members a payoff higher than to what they currently receive under x.

As the *Core* allocation is a set of allocations that are feasible and cannot be improved upon by any coalition, the *Core* allocation is *Pareto* efficient. Therefore, there is no pareto improvement from *Core* allocation. We investigate two most widely used fair allocation methods in this paper which are *Shapley Value* [39] and *Nucleolus* [40].

Definition 4.7. *(Shapley Value)* The Shapley value deals with dividing the surplus among players in a coalition. Given the coalition (v, N), the *Shapley value* for each player $\mathbb{i}$ is calculated as:

$$\phi_{\mathbb{i}}(\mathrm{v}) = \sum_{S \subseteq N \backslash \{\mathbb{i}\}} \frac{|S|!(n - |S| - 1)!}{n!} [\mathrm{v}(S \cup \{\mathbb{i}\}) - \mathrm{v}(S)] \quad (3)$$

Definition 4.8. (*Nucleolus*) *Nucleolus* searches for the allocation which minimizes the worst inequity. As an inequity measure of an allocation x, it uses *excess* value as

$$e(x, S) = \mathrm{v}(S) - \sum_{j \in S} x_j \quad (4)$$

Both *Shapley value* and *Nucleolus* prescribe a unique solution in all cases.

4.3 Coalition Formation

Here, we model the cybersecurity information sharing as a multi-stage coalitional game. The game players are the organizations. The information possessor o_i strategy is to decide whether to share or not to share the information taking into account the reward value $r_{i,k}$. If o_i decides to share the vulnerability information v_k, then its utility is $u_{i,k} = r_{i,k} - \tau_{i,k}$. On the other side, when the vulnerability gets shared then the utility of $o_{j \neq i}$ players are $u_{j,k} = \pi_{j,k} - x_{j,k}$. This game has m stages where m represent the number of vulnerabilities which are being detected in the cybersecurity information sharing cycle. Thus, the characteristic function of this game for each stage is

$$\mathrm{v}(S) = \begin{cases} 0 & |S| = 1 \text{ or } i \notin S \\ \sum_{j \in S} \pi_{j,k} & i \in S \end{cases} \quad (5)$$

Here, the value of a single coalition is equal to 0, this is due to the fact that no information is getting shared between entities. If the information possessor belongs to the coalition, then the value of coalition is equal to the total benefit of organizations existing in the coalition. In this case, the organizations receiving profits from the shared information should pay to the information possessor.

As an example, consider we have $O = \{o_1, o_2, o_3\}$. o_1 detects a vulnerability v_k and shares its feature set F_{v_k} to o_2 and o_3. Then, $\mathcal{S}$ computes the patching benefit of this vulnerability over o_2 and o_3 as $\pi_{2,k} = 5, \pi_{3,k} = 12$. In this case, for $|S| = 1$ or $o_1 \notin S$, no information is getting shared and as a result, the value of coalition is zero. For, $S = \{o_1, o_2\}$, $S = \{o_1, o_3\}$, and $S = \{o_1, o_2, o_3\}$, the coalition values are $v(S) = 5$, $v(S) = 12$, and $v(S) = 17$ respectively.

In this setting, it is trivial that there is no incentive for any subset of the members to separate and form smaller cooperation. In other words, this game is *Superadditive*. In the following, we investigate the *Shapley value* and *Nucleolus* allocations for the cybersecurity information sharing game.

Theorem 4.1 The *Shapley Value* allocation for the cybersecurity information sharing coalitional game is located in the *Core*.

Proof: The Shapley Value solution of a convex game is in the core [45]. Thus we investigate the convexity of the game. As in this game $\mathrm{v}(S \cup T) = \mathrm{v}(S) + \mathrm{v}(T)$ and the value of $\mathrm{v}(S \cap T) \geq 0$, thus the game is convex and the Shapley Value solution is in the core. □

Theorem 4.2 The *Shapley value* of the o_i(information possessor) is half of the total patching benefits of other organizations accessing the information, and the *Shapley value* for $o_{j \neq i}$ is half of its patching benefit from accessing the information in cybersecurity information sharing game.

Proof: First we start from the Shapley Value of the o_i. Let $(S \subseteq N \backslash \{i\}, |S| = p)$, to simplify the proof we use an auxiliary variable $\mathcal{V}_p$ as

$$\mathcal{V}_p = \frac{p!(n - p - 1)!}{n!} \quad (6)$$

Then based on equations (3) and (6) we have

$$\phi_i(\mathrm{v}) = \sum_{p=1}^{n-1} \mathcal{V}_p . \sum_{S \subseteq N \backslash \{i\}} [\mathrm{v}(S \cup \{i\}) - \mathrm{v}(S)]$$

Note that, when $p = n$, then the coalition contains o_i, and thus we do not count this subset. Based on equation (5), $\mathrm{v}(S) = 0$ and the value of $\mathrm{v}(S \cup \{i\})$ is a coefficient of $\sum_j \pi_{j,k}$, in other words $\mathrm{v}(S \cup \{i\}) = \alpha_p \cdot \sum_j \pi_{j,k}$. Hence, we can rewrite $\phi_i(\mathrm{v})$ as

$$\phi_i(\mathrm{v}) = \sum_{p=1}^{n-1} \frac{p!(n - p - 1)!}{n!} \cdot \alpha_p \cdot \sum_j \pi_{j,k}$$

As the number of subsets $(S \subseteq N \backslash \{i\}, |S| = p)$ is $\binom{n-1}{|S|}$ and for each subset S, we have $\frac{p}{n-1}$ benefit values, thus we can calculate α_p as

$$\alpha_p = \binom{n-1}{p} \cdot \frac{p}{n-1}$$

Thus $\phi_i(v)$ is

$$\begin{aligned}
\phi_i(\mathrm{v}) &= \sum_{p=1}^{n-1} \frac{p!(n-p-1)!}{n!} \cdot \binom{n-1}{p} \cdot \frac{p}{n-1} \cdot \sum_j \pi_{j,k} \\
&= \sum_{p=1}^{n-1} \frac{p!(n-p-1)!(n-1)! \cdot p}{n!p!(n-p-1)! \cdot (n-1)} \cdot \sum_j \pi_{j,k} \\
&= \sum_{p=1}^{n-1} \frac{p}{n(n-1)} \cdot \sum_j \pi_{j,k} \\
&= \frac{1}{n(n-1)} \sum_{p=1}^{n-1} p \cdot \sum_j \pi_{j,k} \\
&= \frac{1}{n(n-1)} \cdot \frac{n(n-1)}{2} \cdot \sum_j \pi_{j,k} \\
&= \frac{1}{2} \cdot \sum_j \pi_{j,k}
\end{aligned}$$

Now we compute o_j's Shapley Value. For o_j, we need to count the subsets S containing o_i, since the coalition values for other subsets are zero. In this case, we have $[\mathrm{v}(S \cup \{j\}) - \mathrm{v}(S)] = \pi_{j,k}$. Thus, we have $\sum_{S \subseteq N \setminus \{i\}} [\mathrm{v}(S \cup \{j\}) - \mathrm{v}(S)] = \beta_p \cdot \pi_{j,k}$, where β_p is the number of subsets $\{S \subseteq N \setminus \{j\}, \{i\} \in S, |S| = p\}$ which is

$$\beta_p = \binom{n-2}{p-1}$$

Thus we have

$$\begin{aligned}
\phi_j(\mathrm{v}) &= \sum_{p=1}^{n-1} \frac{p!(n-p-1)!}{n!} \cdot \binom{n-2}{p-1} \cdot \pi_{j,k} \\
&= \sum_{p=1}^{n-1} \frac{p!(n-p-1)!(n-2)!}{n!(p-1)!(n-p-1)!} \cdot \pi_{j,k} \\
&= \sum_{p=1}^{n-1} \frac{p}{n(n-1)} \cdot \pi_{j,k} \\
&= \frac{1}{n(n-1)} \sum_{p=1}^{n-1} p \cdot \pi_{j,k} \\
&= \frac{1}{n(n-1)} \cdot \frac{n(n-1)}{2} \cdot \pi_{j,k} \\
&= \frac{1}{2} \cdot \pi_{j,k}
\end{aligned}$$

□

Theorem 4.3 The *Shapley value* and *Nucleolus* solution concepts, coincide in the cybersecurity information sharing game.

Proof:
In order to proof this theorem, we calculate the excess value in equation (4) with the Shapley Value allocation. Let o_i indicate the information possessor and $o_{j \neq i}$ represent other organizations. For subsets $|S| = 1$ and $i \notin S$, the coalition value is zero $\mathrm{v}(S) = 0$ and we have $\sum_{j \in S} x_j = 0$, thus we have $e(x, S) = 0$. For the remain subsets, according to theorem 4.2 o_i's allocation is $\frac{1}{2} \sum_{j \in S} \pi_{j,k}$ and o_j' allocation is $\frac{1}{2}\pi_{j,k}$. By replacing the coalition value according to equation (5) characteristic function, we have

$$\begin{aligned}
e(x, S) &= \mathrm{v}(S) - (x_i + \sum_{j \in S} x_j) \\
&= \sum_{j \in S} \pi_{j,k} - (\frac{1}{2} \sum_{j \in S} \pi_{j,k} + \sum_{j \in S} \frac{1}{2} \pi_{j,k}) = 0
\end{aligned}$$

As the excess value for all of the subsets are equal to zero and since Nucleolus present a unique solution, then we conclude that the solution concepts of the Shapley Value and Nucleolus coincide in the cybersecurity information sharing game.

□

So far we have analyzed the fair profit sharing in cybersecurity information sharing. However, as the participation-fee reveals sensitive information about the organizations' cyber-infrastructure, in the next section we propose a method to protect participation-fee.

5 Differentially Private Rewarding

As the organizations' participation-fee in the cybersecurity information sharing rewarding system reveals sensitive information about the organizations' cyber-infrastructure, and such information can be exploited by the attackers to exploit the organizations' vulnerabilities, it is critical to protecting the organizations' participation-fee. To this end, in this section, we propose a differentially private mechanism for cybersecurity information sharing coalitional game. First, we describe the differential privacy and the methods for achieving this requirement. Then, we analyze the security requirements for cybersecurity information sharing. Finally, we propose our algorithm and check if it fulfills the differential privacy requirement.

5.1 Differential Privacy

The notion of differential privacy [32] was first introduced in the statistical database to hide sensitive private data in aggregate statistical information. Roughly speaking, the goal of differential privacy is to allow learning useful information about a population in the database while protecting an individual's information. By applying differential privacy, the responses to the queries are independent of the presence or absence of an individual in the database. This method applies a randomized response to prevent an adversary armed with background information to infer the existence of an individual in the database with a probability. Formally we can define the differential privacy as follows

Definition 5.1. (*Differential privacy*) [32] Let $D \in \mathbb{N}^{|\mathcal{U}|}$ denote a collection of records from a universe $\mathcal{U}$. A randomized algorithm $\mathcal{M}(\mathcal{D})$ is ϵ-differentially private if for any set of possible output $\mathcal{O} \subseteq$ Range($\mathcal{M}$) and for any adjacent databases $D, D' \in \mathbb{N}^{|\mathcal{U}|}$ such that $||D - D'||_1 \leq 1$ (D, D' known as neighbor databases which only differ in one record), we have

$$\Pr[\mathcal{M}(\mathcal{D}) \in \mathcal{O}] \leq e^{\epsilon} \times \Pr[\mathcal{M}(\mathcal{D}') \in \mathcal{O}] \qquad (7)$$

In this definition, ϵ is known as the privacy budget. The smaller value of ϵ leading stricter indistinguishability and improves privacy. In words, Definition 5.1 indicates that by having access to the differentially private mechanism output, it is unlikely to distinguish which of two neighboring databases are given as input to the mechanism. There are two well-known tools to provide differential privacy as described in the following.

1) *The Laplace Mechanism* [32]

In this technique, a noise value is appended to the output to hide the original value. One way to calculate the noise is to sample it from the Laplace distribution. In this case, first, the global sensitivity rate is measured. Given any function $f : \mathbb{N}^{|\mathcal{U}|} \to \mathcal{O}$, the global sensitivity of f is defined as

$$\Delta f = \max_{\substack{D,D' \in \mathbb{N}^{|\mathcal{U}|} \\ ||D-D'||_1=1}} ||f(D) - f(D')||_1 \quad (8)$$

Then, the Laplace mechanism calculates the output as follows

$$\mathcal{M}(D, f(.), \epsilon) = f(D) + \text{Lap}(\Delta f/\epsilon) \quad (9)$$

2) *The Exponential Mechanism*[34]

The exponential mechanism chooses output with probability considering the utility of output while preserving the result differentially private. More precisely, let $u(D, O) : (\mathbb{N}^{|\mathcal{U}|} \times \mathcal{O}) \rightarrow R$ represent the utility function receiving the database and mechanism output value as input and returns the utility score. Let's define Δu as

$$\Delta u = \max_{\substack{D,D':||D-D'||_1 \leq 1 \\ O \in \mathcal{O}}} |u(D, O) - u(D', O)| \quad (10)$$

Then, the mechanism $\mathcal{M}(D, u)$ is ϵ-differentially private if it returns O with probability proportional to $exp(\frac{\epsilon u(D,O)}{2\Delta u})$.

5.2 Private Rewarding Mechanism

In the fair and private rewarding mechanism, as we want to keep the fairness property, we apply the exponential mechanism to preserve the fairness quality. The Laplace mechanism can not directly be applied in cybersecurity information sharing rewarding, because the global sensitivity range can be large causing the noise value increases substantially and as a result, the participation-fee might get larger than the patching benefit. Hence, we apply the *exponential mechanism.*

In order to apply the *exponential mechanism*, first, we need to define the utility function. As our mechanism needs to fulfill fairness along with the privacy, we define the utility function considering fairness. To this end, we relax the fairness allocation presented in the profit sharing by defining δ-fairness.

Definition 5.2. Let $\Psi = (\psi_1, , ..., \psi_n)$ represent the fair allocation, then the allocation $\bar{x} = (x_1, ..., x_n)$ is δ-fair if for all x_i, we have $x_i \in (\psi_i - \delta, \psi_i + \delta)$.

According to δ-fairness definition, and the fair profit sharing discussed in section 4, in the cybersecurity information sharing rewarding, for the information possessor o_i, an allocation x_i is δ-fair if we have $x_i \in (1/2 \sum_j \pi_j - \delta, 1/2 \sum_j \pi_j + \delta)$, and for o_j exploiting the patching benefit, an allocation x_j is δ-fair if we have $x_j \in (1/2\pi_j - \delta, 1/2\pi_j + \delta)$.

Note that, δ value should be chosen in a way to fulfill the differential privacy requirement. More precisely, when the probability of output for a mechanism over a database input is larger than zero, then the probability of output for the mechanism over the adjacent database should also be larger than zero. Formally we have

$$(\Pr[\mathcal{M}(\mathcal{D}) \in \mathcal{O}] > 0) \Rightarrow (\Pr[\mathcal{M}(\mathcal{D}') \in \mathcal{O}] > 0) \quad (11)$$

To meet this requirement, the δ value should be chosen such that if the most effective element in the database is removed then the probability of mechanism output is still larger than zero. Formally we have

$$\begin{aligned} & \hat{x} < \sum_{n-2} \delta \\ & s.t. \quad \hat{x} \in D, \hat{x} = \arg \quad \max ||M(D) - M(D - \hat{x})||_1 \end{aligned} \quad (12)$$

This requirement indicates that with the increasing of the input values variance and also with the decreasing of the number of input elements, δ value should be increased, which results in the increasing of fairness cost.

As the randomized response is changing the fair profit sharing, we are interested in finding the δ-fair private profit sharing. Our proposed mechanism has two parts. In the first part, we deal with finding the private and δ-fair reward value, and in the second part, we investigate the private and δ-fair cost division among participants.

Let $\mathbb{X} = (x_1, ..., x_n)$ represent the profit allocation given the allocation of information possessor $x_i = r_i$. The algorithm (1) takes as input the privacy budget ϵ and the fair profit sharing vector $\Psi = (\psi_1, ..., \psi_n)$ (which is $\psi_j = \pi_j/2$ and $\psi_i = \sum_j \pi_j/2$ in cybersecurity information sharing), and obtains the private δ-fair reward r_i as output.

In the beginning, δ value is selected in such a way to fulfill the requirement (12). As the goal of the privacy preserving algorithm is to retain fairness as much as possible, we define the utility function as follows

$$u(\Psi, \mathbb{X}) = \frac{1}{||\mathbb{X} - \Psi||_1 + 1} \quad (13)$$

In this definition, we consider the increasing of distance between profit allocation and fair profit sharing decrease the utility. As the maximum value of utility is obtained in Ψ allocation, then according to equation (10) we have

$$\begin{aligned} \Delta u(\Psi, \mathbb{X}) &= \frac{1}{||\Psi - \Psi||_1 + 1} - \frac{1}{max(\psi_j) + 1} \\ &= 1 - \frac{1}{max(\psi_j) + 1} = \frac{max(\psi_j)}{max(\psi_j) + 1} \end{aligned} \quad (14)$$

To meet the δ-fair requirement, the candidate reward values are taken from $(\psi_i - \delta, \psi_i + \delta)$ range. Then, the probability distribution of different values for reward is calculated and the output is sampled from the following distribution.

$$Pr[r_i = x_i] = \frac{exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbb{X}-\Psi||_1+1).max(\psi_j)})}{\sum_{x_i \in (\psi_i-\delta,\psi_i+\delta)} exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbb{X}-\Psi||_1+1).max(\psi_j)})} \quad (15)$$

This distribution is chosen to fulfill the differential privacy requirement as discussed in theorem 5.1. Note that, with the decrease of the distance to fair allocation, the probability increases exponentially. This makes the distribution to be biased toward fair profit sharing while fulfilling the differential privacy requirement.

Theorem 5.1 Algorithm (1) is δ-fair and ϵ-differentially private.

Proof: It is trivial that Algorithm (1) is δ-fair as the range of samples is $(\psi_i - \delta, \psi_i + \delta)$. In order to prove ϵ-differential privacy, we investigate the probability of having the same output for two neighbor profiles $\mathbb{X}, \mathbb{X}'$. We sketch the proof from [46]. Thus we have

(Note that, $||\mathbb{X} - \Psi||_1 - ||\mathbb{X}' - \Psi||_1 \leq max(\psi_j)$.)

$$\begin{aligned} \frac{Pr[Alg1(\mathbb{X}) = r]}{Pr[Alg1(\mathbb{X}') = r]} &= \frac{exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbb{X}-\Psi||_1+1).max(\psi_j)})}{exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbb{X}'-\Psi||_1+1).max(\psi_j)})}. \\ & \frac{\sum_{x_i \in (\psi_i-\delta,\psi_i+\delta)} exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbb{X}'-\Psi||_1+1).max(\psi_j)})}{\sum_{x_i \in (\psi_i-\delta,\psi_i+\delta)} exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbb{X}-\Psi||_1+1).max(\psi_j)})} \\ &= exp(\frac{\epsilon.(\frac{1}{||\mathbb{X}-\Psi||_1+1} - \frac{1}{||\mathbb{X}'-\Psi||_1+1})}{2.\frac{max(\psi_j)}{max(\psi_j+1)}}). \\ & \frac{\sum_{x_i \in (\psi_i-\delta,\psi_i+\delta)} exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbb{X}'-\Psi||_1+1).max(\psi_j)})}{\sum_{x_i \in (\psi_i-\delta,\psi_i+\delta)} exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbb{X}-\Psi||_1+1).max(\psi_j)})} \\ &\leq exp(\frac{\epsilon}{2}).exp(\frac{\epsilon}{2}). \\ & \frac{\sum_{x_i \in (\psi_i-\delta,\psi_i+\delta)} exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbb{X}-\Psi||_1+1).max(\psi_j)})}{\sum_{x_i \in (\psi_i-\delta,\psi_i+\delta)} exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbb{X}-\Psi||_1+1).max(\psi_j)})} \\ &= exp(\epsilon) \end{aligned}$$

Hence we can rewrite the probabilities as follows

$$Pr[Alg1(\mathbb{X}) = r] \leq exp(\epsilon).Pr[Alg1(\mathbb{X}') = r]$$

□

Algorithm 1: Randomized algorithm for finding the differentially private reward value

```
Input  : Privacy budget $\epsilon$, fairness threshold $\delta$, and fair profit
         sharing vector $\Psi$
Output: The randomized private $\delta$-fair reward value $r_i$
$S \leftarrow 0$;
foreach $x_i \in (\psi_i - \delta, \psi_i + \delta)$ do
    $S \leftarrow S + exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbb{X}-\Psi||_1+1).max(\psi_j)})$;
end
Sample $r_i$ from the following distribution
    $\Pr[r_i = x_i] = \frac{exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbb{X}-\Psi||_1+1).max(\psi_j)})}{S}$
return $r_i$;
```

In the next algorithm, we apply differential privacy to privately divide the cost of reward into the organizations considering their patching benefits. Note that, if we divide the cost fairly, this problem is a particular instance of the airport cost allocation game [47]. In this case, the adversary with side information and the collusion of organizations reveals the victim's patching benefit. Thus, in algorithm (2) we randomize the cost to preserve the differential privacy. In this case, we model the utility function as follows

$$u(\mathbb{X}, \mathbb{Y}) = \frac{1}{||\mathbb{Y} - \mathbb{X}||_1 + 1} \tag{16}$$

Having this definition, with the increase of distance of allocation and As the maximum utility is obtained in $\mathbb{Y} = \mathbb{X}$, then Δu is

$$\begin{aligned}\Delta u(\mathbb{X}, \mathbb{Y}) &= \frac{1}{||\mathbb{X} - \mathbb{X}||_1 + 1} - \frac{1}{||\mathbb{X} - (\mathbb{X} - max(x_j))||_1 + 1} \\ &= 1 - \frac{1}{max(x_j) + 1} = \frac{max(x_j)}{max(x_j) + 1} \end{aligned} \tag{17}$$

Algorithm (2) takes the profit sharing vector $\mathbb{X}$ with $x_i = r_i$, the fairness threshold value δ, and the original fair profit sharing vector Ψ as input, and generates the private δ-fair profit sharing allocation vector $\mathbb{Y} = (y_1, ..., y_n)$ as output such that $y_i = r_i$.

In algorithm (2), every possible combination of participation-fees leading to the reward value r_i, as it can be seen in line 3. The combinations of participation-fees make the samples of the distribution. Afterward, the probability distribution is calculated and the participation-fee vector is sampled from the following distribution to fulfill the differential privacy requirement as discussed in theorem 5.2.

$$Pr[\mathbb{Y} = \mathbf{m}] = \frac{exp(\frac{\epsilon.(max(x_j)+1)}{2.(||\mathbf{m}-\mathbb{X}||_1+1).max(x_j)})}{\sum_{\forall \mathbf{m} \in \mathbb{M}} exp(\frac{\epsilon.(max(x_j)+1)}{2.(||\mathbf{m}-\mathbb{X}||_1+1).max(x_j)})} \tag{18}$$

Theorem 5.2 Algorithm (2) is δ-fair and ϵ-differentially private.

Proof: The proof is almost the same as that of Theorem 5.1. As the elements of the matrix M is chosen from the range of $(\psi_j - \delta, \psi_j + \delta)$, algorithm (2) is δ-fair. Let $\mathbb{X}$ and $\mathbb{X}'$ be neighbor payment profiles, then we have

(Note that, $||\mathbf{m} - \mathbb{X}||_1 - ||\mathbf{m} - \mathbb{X}'||_1 \leq max(x_j)$.)

$$\begin{aligned}\frac{Pr[Alg2(\mathbb{X}) = \mathbb{Y}]}{Pr[Alg2(\mathbb{X}') = \mathbb{Y}]} &= \frac{exp(\frac{\epsilon.(max(x_j)+1)}{2.(||\mathbb{Y}-\mathbb{X}||_1+1).max(x_j)})}{exp(\frac{\epsilon.(max(x_j)+1)}{2.(||\mathbb{Y}-\mathbb{X}'||_1+1).max(x_j)})}. \\ &\quad \frac{\sum_{\mathbf{m}\in\mathbb{M}} exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbf{m}-\mathbb{X}'||_1+1).max(\psi_j)})}{\sum_{\mathbf{m}\in\mathbb{M}} exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbf{m}-\mathbb{X}||_1+1).max(\psi_j)})} \\ &= exp(\frac{\epsilon.(\frac{1}{||\mathbf{m}-\mathbb{X}||_1+1} - \frac{1}{||\mathbf{m}-\mathbb{X}'||_1+1})}{2.\frac{max(\psi_j)}{max(\psi_j+1)}}). \\ &\quad \frac{\sum_{\mathbf{m}\in\mathbb{M}} exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbf{m}-\mathbb{X}'||_1+1).max(\psi_j)})}{\sum_{\mathbf{m}\in\mathbb{M}} exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbf{m}-\mathbb{X}||_1+1).max(\psi_j)})} \\ &\leq exp(\frac{\epsilon}{2}).exp(\frac{\epsilon}{2}). \\ &\quad \frac{\sum_{\mathbf{m}\in\mathbb{M}} exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbf{m}-\mathbb{X}||_1+1).max(\psi_j)})}{\sum_{\mathbf{m}\in\mathbb{M}} exp(\frac{\epsilon.(max(\psi_j)+1)}{2.(||\mathbf{m}-\mathbb{X}||_1+1).max(\psi_j)})} \\ &= exp(\epsilon)\end{aligned}$$

Hence we can rewrite the probabilities as follows

$$Pr[Alg2(\mathbb{X}) = \mathbb{Y}] \leq exp(\epsilon).Pr[Alg2(\mathbb{X}') = \mathbb{Y}]$$

□

Algorithm 2: Randomized algorithm for finding the differentially private reward value

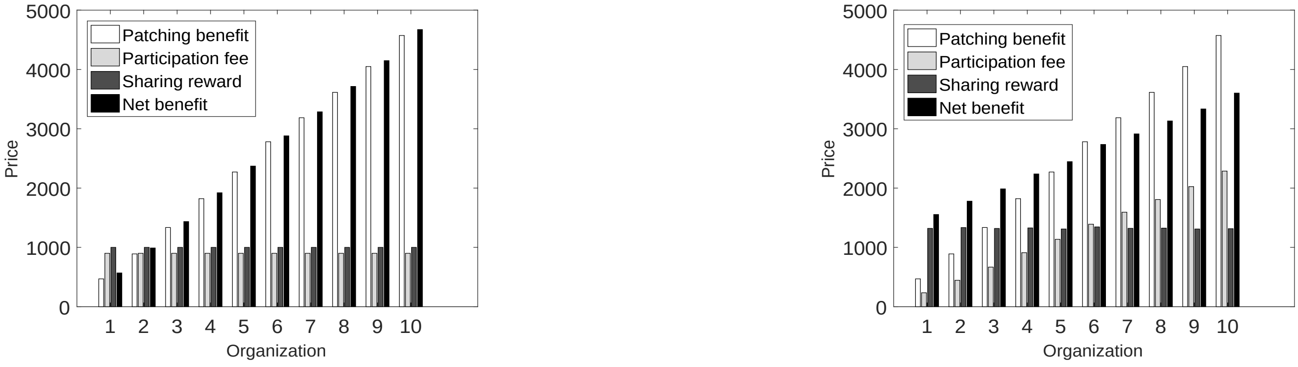
```
  Input  : The fair cost allocation vector $\mathbb{X}$ with $x_i = r_i$, the
           fairness threshold value $\delta$, and the original fair
           profit sharing vector $\Psi$
  Output: The randomized private $\delta$-fair patching benefit
           vector $\mathbb{Y}$
1 $S \leftarrow 0$
2 Initialize matrix $\mathbb{M}$'s rows to all of possible combinations of
    the cost allocations such that for each row vector m we have
    $a_{i,m} = r_i$, $a_{j,m} \in (\psi_j - \delta, \psi_j + \delta)$, and $\sum_j a_{j,m} = r_i$.
3 foreach row vector m $\in \mathbb{M}$ do
4     $S \leftarrow S + exp(\frac{\epsilon.(max(x_j)+1)}{2.(||\mathbf{m}-\mathbb{X}||_1+1).max(x_j)})$;
5 end
6 Sample $\mathbb{Y}$ from the following distribution
    $\Pr[\mathbb{Y} = \mathbf{m}] = \frac{exp(\frac{\epsilon.(max(x_j)+1)}{2.(||\mathbf{m}-\mathbb{X}||_1+1).max(x_j)})}{S}$
7 return $\mathbb{Y}$;
```

6 Simulation Results

In this section, we investigate the performance of our proposed mechanisms. First, we evaluate the effect of applying coalitional game theory model introduced in section 4 for reward/participation-fee allocation on cybersecurity information sharing system. Afterward, we analyze the private reward/participation-fee allocation as presented in section 5.

6.1 Fair Rewarding

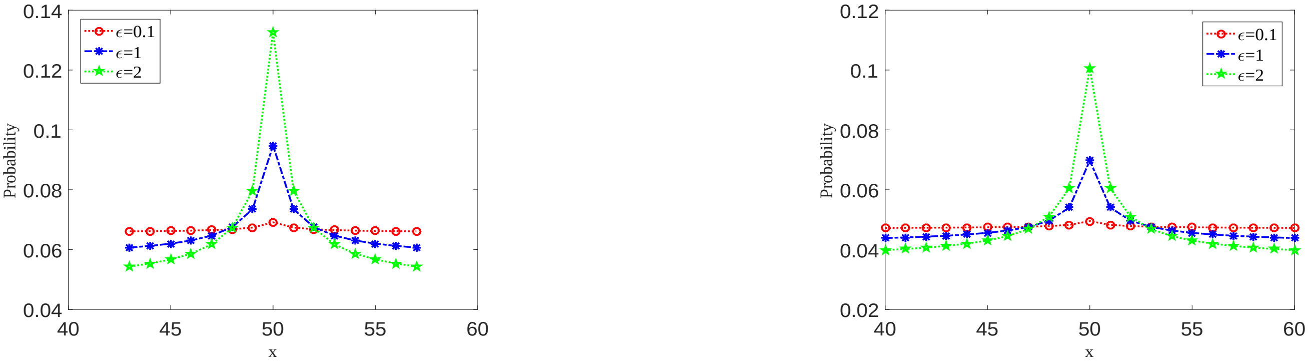
Here, we compare our proposed game-theoretic mechanism discussed in section 4 with the static allocation where participation-fee and reward are constant values for all of the organizations and



(a) Non-game-theoretic approach

(b) Game-theoretic approach

Fig. 3: Comparing the game-theoretic and non-game-theoretic approaches



(a) Sampling distribution for $\delta = 7$

(b) Sampling distribution for $\delta = 10$

Fig. 4: Comparing sampling distributions with $\delta = 7$ and $\delta = 10$

every vulnerability information sharing. The goal of this experiment is to study the benefits of applying the coalitional game theoretic approach comparing to a static reward/participation-fee allocation scheme. We set the number of organizations to $n = 10$ and the number of vulnerabilities to $m = 100$. We assume each vulnerability randomly detected by an organization and the rest of organizations are vulnerable with probability 0.5. Organizations are sorted in the list based on their size in terms of their patching benefit $\pi_{j,k}$ (e.g. o_{10} is the largest organization and o_1 is the smallest organization). We assume the patching benefit is proportional to the organization's size and we calculate it as $\pi_{j,k} \sim \mathcal{N}(j \times 10, 5)$.

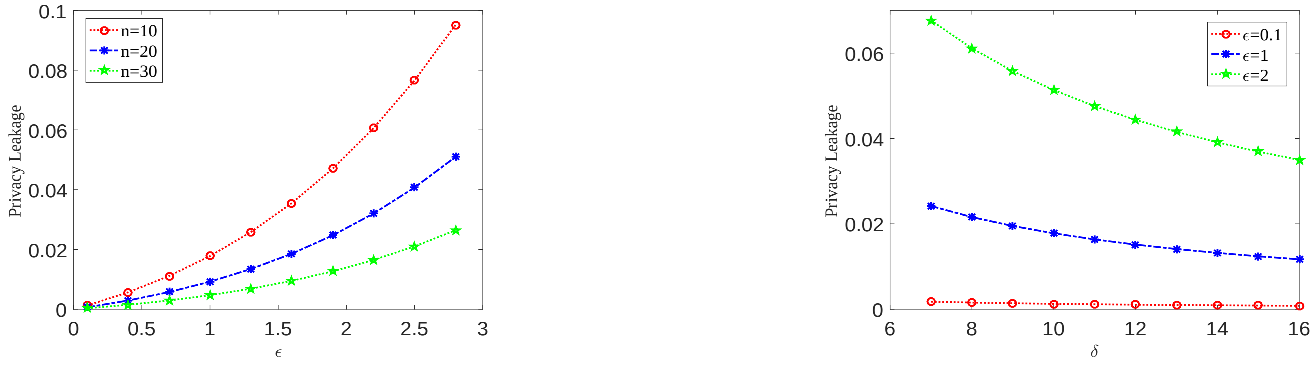
In the static model, we consider $r_{i,k} = 100, x_{j,k} = 20$. Figure 3b shows the improvement achieved by game-theoretic formation as compared to the non-game-theoretic approach as depicted in Figure 3a. We calculate *net-benefit* value as the summation of patching benefit and sharing reward deducted by the participation-fee. As it can be seen, using the game-theoretic approach results in better distribution of the payoff among organizations while in the non-game-theoretic model the larger organizations benefit more from the system. It is due to the fact that in the non-game-theoretic setting, participation-fee is same for all of the organizations without consideration of their benefit from the system, while in the game-theoretic approach, the participation-fee is dynamically calculated based on the patching benefit. Besides that, as the reward value in the game-theoretic method is dynamically calculated based on the patching benefit, organizations are stimulated to share more useful information to the system. In our simulation, the game-theoretic approach results in higher rewards comparing to the non-game-theoretic approach. We have used MatTuGames [48] to implement the proposed profit-sharing model.

6.2 Differentially Private Rewarding

Here, we analyze the performance of the differentially private profit sharing algorithms introduced in section 5. For this purpose, we measure the changes of *privacy-leakage* and *fairness-distance* when other parameters vary. We calculate *privacy-leakage* through *Kullback-Leibler (KL) divergence* [49]. KL divergence computes the difference between two distributions. Let D, D' represent two neighbor databases differ in only one organization participating in the rewarding process, and Q, Q' indicate the probability of patching benefit distribution, correspondingly. Since by increasing the difference of these distributions, the databases are more distinguishable, we define the privacy-leakage to be calculated as KL divergence as follows

$$D(Q||Q') = \sum_{y \in \mathbb{Y}} Q(y) ln(\frac{Q(y)}{Q'(y)}) \tag{19}$$

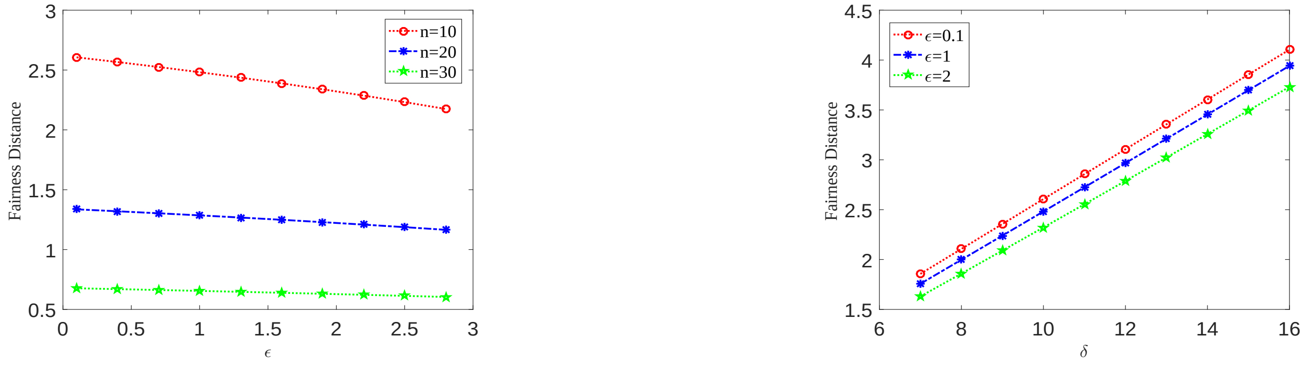
Figure 4 illustrates the sampling distributions where $n = 10$ and $x = 50$ for $\delta = 7$ and $\delta = 10$. Note that, in this case, the δ value should be larger than seven according to requirement (12). It can be seen that the increase of δ value provides more privacy by distributing sample space and decreasing the probability of sample selection as a result. Also, with the decrease of the distance to fair allocation, the probability increases exponentially. This makes the distribution to be biased toward fair profit sharing while fulfilling the differential privacy requirement. On the other hand, figure 5 displays the impacts of δ, ϵ, and n on privacy leakage. As it can be observed, by increasing the privacy budget ϵ, the privacy leakage increase but at the decreasing rate. Moreover, with the growth of the number of organizations in the coalition, the privacy leakage decreases. This is in light of the fact that with the growth of organizations coalition the sample space is also growing as indicated in equations (15), and (18).



(a) Privacy leakage with the increase of ϵ

(b) Privacy leakage with the increase of δ

Fig. 5: Privacy leakage with the increasing of δ and ϵ



(a) Fairness distance with the increase of ϵ

(b) Fairness distance with the increase of δ

Fig. 6: Fairness distance with the increasing of δ and ϵ

In order to calculate the *fairness*, we calculate the distance between the fair profit sharing vector Ψ and the expected profit allocation vector $\mathbb{Y}$ from our algorithms output, and then we divide the result by the number of participating organizations to calculate the average distance. Figure 6 shows the impacts of δ, ϵ, and n on fairness distance. The distance from fair allocation is decreasing with an increase of organizations number and an increase of ϵ. On the other hand, increasing the δ value, increase the fairness distance linearly. As a result, it can be concluded that the increase of the number of organizations participating in the cybersecurity information sharing coalition, the value of patching benefit, and δ yield better performance of our algorithm. Moreover, the algorithm provides a better result when the patching benefits variance is small.

7 Conclusion

Despite the benefits of sharing cybersecurity information, stimulating organizations to share their cybersecurity information is a big challenge. As such sharing is costly, organizations tend to free-ride in the system and as a result, useful information is not getting shared. To motivate sharing behavior, we have proposed a reward/participation-fee allocation mechanism based on coalitional game theory. We have also investigated the *Shapley value* and *Nucleolus* solution concepts of cybersecurity information sharing as a coalitional game to reach a fair, dynamic, and stable profit sharing method. On the other hand, as a participation-fee reveals sensitive information about the organizations' cyberstructure, we have investigated the private and fair rewarding mechanism applying the differential privacy concept. We relax the fairness definition by introducing δ-fair concept. Then, we have offered a private and δ-fair profit allocation mechanism. The simulation results depict the efficiency of our proposed mechanism.

For future works, we are interested in modeling a cybersecurity information sharing platform as a self-driven public-good market, where the organizations' participation-fee motivates data holders to share useful information. In such a market, organizations can bid for their required cybersecurity information based on their true valuations. On the other hand, the vulnerability finder decides whether to sell the information to the organizations or sell it to the attackers in the black market. In this game, we would like to investigate the Nash Equilibrium and design mechanisms to motivate organizations toward the socially optimal point where useful information is getting shared and organizations' best strategy is to invest on cybersecurity.

8 Acknowledgments

This research is partially supported by the National Science Foundation (NSF), USA, Award #1528167. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

9 References

1 Brown, S., Gommers, J., Serrano, O. 'From cyber security information sharing to threat management'. In: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. (ACM, 2015. pp. 43–49)
2 Fischer, E., Liu, E., Rollins, J., Theohary, C.: 'The 2013 cybersecurity executive order: Overview and considerations for congress', , 2013,
3 'S.754 - to improve cybersecurity in the united states through enhanced sharing of information about cybersecurity threats, and for other purposes.', https://www.congress.gov/bill/114th-congress/senate-bill/754/'.
4 'Cyber-security information sharing partnership (cisp)', https://www.ncsc.gov.uk/cisp'.

5 'Cyber security information sharing: An overview of regulatory and non-regulatory approaches', https://www.enisa.europa.eu/publications/cybersecurity-information-sharing'.

6 Gordon, L.A., Loeb, M.P., Lucyshyn, W.: 'Sharing information on computer systems security: An economic analysis', *Journal of Accounting and Public Policy*, 2003, **22**, (6), pp. 461–485

7 Gal.Or, E., Ghose, A.: 'The economic incentives for sharing security information', *Information Systems Research*, 2005, **16**, (2), pp. 186–208

8 Khouzani, M., Pham, V., Cid, C. 'Strategic discovery and sharing of vulnerabilities in competitive environments'. In: International Conference on Decision and Game Theory for Security. (Springer, 2014. pp. 59–78)

9 Rapoport, A., Chammah, A.M.: 'Prisoner's dilemma: A study in conflict and cooperation'. vol. 165. (University of Michigan press, 1965)

10 Moore, T., Dynes, S., Chang, F.R.: 'Identifying how firms manage cybersecurity investment', *Available: Southern Methodist University Available at: http://blog smu edu/research/files/2015/10/SMU-IBM pdf (Accessed 2015-12-14)*, 2015, **32**

11 Vakilinia, I., Sengupta, S. 'A coalitional game theory approach for cybersecurity information sharing'. In: Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE. (IEEE, 2017. pp. 237–242)

12 Rutkowski, A., Kadobayashi, Y., Furey, I., Rajnovic, D., Martin, R., Takahashi, T., et al.: 'Cybex: The cybersecurity information exchange framework (x. 1500)', *ACM SIGCOMM Computer Communication Review*, 2010, **40**, (5), pp. 59–64

13 Laube, S., Böhme, R.: 'The economics of mandatory security breach reporting to authorities', *Journal of Cybersecurity*, 2016, p. tyw002

14 Steinberger, J., Sperotto, A., Golling, M., Baier, H. 'How to exchange security events? overview and evaluation of formats and protocols'. In: Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on. (IEEE, 2015. pp. 261–269)

15 Kampanakis, P.: 'Security automation and threat information-sharing options', *Security & Privacy, IEEE*, 2014, **12**, (5), pp. 42–51

16 Khalili, M.M., Naghizadeh, P., Liu, M. 'Embracing risk dependency in designing cyber-insurance contracts'. In: Communication, Control, and Computing (Allerton), 2017 55th Annual Allerton Conference on. (IEEE, 2017. pp. 926–933)

17 Vakilinia, I., Sengupta, S.: 'A coalitional cyber-insurance framework for a common platform', *IEEE Transactions on Information Forensics and Security*, 2018,

18 Khalili, M.M., Naghizadeh, P., Liu, M. 'Designing cyber insurance policies in the presence of security interdependence'. In: Proceedings of the 12th workshop on the Economics of Networks, Systems and Computation. (ACM, 2017. p. 7)

19 Liu, D., Ji, Y., Mookerjee, V.: 'Knowledge sharing and investment decisions in information security', *Decision Support Systems*, 2011, **52**, (1), pp. 95–107

20 Vakilinia, I., Cheung, S., Sengupta, S. 'Sharing susceptible passwords as cyber threat intelligence feed'. In: Military Communications Conference (MILCOM), MILCOM 2018-2018 IEEE. (IEEE, 2018. pp. 1–6)

21 Bhatia, J., Breaux, T.D., Friedberg, L., Hibshi, H., Smullen, D. 'Privacy risk in cybersecurity data sharing'. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. (ACM, 2016. pp. 57–64)

22 Garrido.Pelaz, R., González.Manzano, L., Pastrana, S. 'Shall we collaborate?: A model to analyse the benefits of information sharing'. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. (ACM, 2016. pp. 15–24)

23 Tosh, D.K., Sengupta, S., Mukhopadhyay, S., Kamhoua, C.A., Kwiat, K.A. 'Game theoretic modeling to enforce security information sharing among firms'. In: Cyber Security and Cloud Computing (CSCloud), 2015 IEEE 2nd International Conference on. (IEEE, 2015. pp. 7–12)

24 Tosh, D., Sengupta, S., Kamhoua, C., Kwiat, K., Martin, A. 'An evolutionary game-theoretic framework for cyber-threat information sharing'. In: Communications (ICC), 2015 IEEE International Conference on. (IEEE, 2015. pp. 7341–7346)

25 Vakilinia, I., Tosh, D.K., Sengupta, S. '3-way game model for privacy-preserving cybersecurity information exchange framework'. In: Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE. (IEEE, 2017. pp. 829–834)

26 Vakilinia, I., Tosh, D.K., Sengupta, S. 'Privacy-preserving cybersecurity information exchange mechanism'. In: Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2017 International Symposium on. (IEEE, 2017. pp. 1–7)

27 Halpern, J., Teague, V. 'Rational secret sharing and multiparty computation'. In: Proceedings of the thirty-sixth annual ACM symposium on Theory of computing. (ACM, 2004. pp. 623–632)

28 Goldman, C.V., Zilberstein, S. 'Optimizing information exchange in cooperative multi-agent systems'. In: Proceedings of the second international joint conference on Autonomous agents and multiagent systems. (ACM, 2003. pp. 137–144)

29 Lindell, Y., Pinkas, B.: 'Secure multiparty computation for privacy-preserving data mining', *Journal of Privacy and Confidentiality*, 2009, **1**, (1), pp. 5

30 Brakerski, Z., Vaikuntanathan, V.: 'Efficient fully homomorphic encryption from (standard) lwe', *SIAM Journal on Computing*, 2014, **43**, (2), pp. 831–871

31 Kargupta, H., Datta, S., Wang, Q., Sivakumar, K. 'On the privacy preserving properties of random data perturbation techniques'. In: Data Mining, 2003. ICDM 2003. Third IEEE International Conference on. (IEEE, 2003. pp. 99–106)

32 Dwork, C. 'Differential privacy: A survey of results'. In: International Conference on Theory and Applications of Models of Computation. (Springer, 2008. pp. 1–19)

33 McSherry, F., Mironov, I. 'Differentially private recommender systems: Building privacy into the netflix prize contenders'. In: Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining. (ACM, 2009. pp. 627–636)

34 McSherry, F., Talwar, K. 'Mechanism design via differential privacy'. In: Foundations of Computer Science, 2007. FOCS'07. 48th Annual IEEE Symposium on. (IEEE, 2007. pp. 94–103)

35 Jin, H., Su, L., Ding, B., Nahrstedt, K., Borisov, N. 'Enabling privacy-preserving incentives for mobile crowd sensing systems'. In: Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on. (IEEE, 2016. pp. 344–353)

36 Ács, G., Castelluccia, C. 'I have a dream!(differentially private smart metering).'. In: Information hiding. vol. 6958. (Springer, 2011. pp. 118–132)

37 Backes, M., Meiser, S. 'Differentially private smart metering with battery recharging'. In: Data Privacy Management and Autonomous Spontaneous Security. (Springer, 2014. pp. 194–212)

38 Friedman, A., Sharfman, I., Keren, D., Schuster, A. 'Privacy-preserving distributed stream monitoring.'. In: NDSS. 2014.

39 Shapley, L.S.: 'A value for n-person games', *Contributions to the Theory of Games*, 1953, **2**, (28), pp. 307–317

40 Schmeidler, D.: 'The nucleolus of a characteristic function game', *SIAM Journal on applied mathematics*, 1969, **17**, (6), pp. 1163–1170

41 Saad, W., Han, Z., Debbah, M., Hjorungnes, A., Basar, T.: 'Coalitional game theory for communication networks', *IEEE Signal Processing Magazine*, 2009, **26**, (5), pp. 77–97

42 Singh, C., Sarkar, S., Aram, A., Kumar, A.: 'Cooperative profit sharing in coalition-based resource allocation in wireless networks', *IEEE/ACM Transactions on Networking (TON)*, 2012, **20**, (1), pp. 69–83

43 Cai, J., Pooch, U. 'Allocate fair payoff for cooperation in wireless ad hoc networks using shapley value'. In: Parallel and distributed processing symposium, 2004. Proceedings. 18th International. (IEEE, 2004. p. 219)

44 Muto, S., NAKAYAMA, M., POTTERS, J., TIJS, S.: 'On big boss games', *The Economic Studies Quarterly*, 1988, **39**, (4), pp. 303–321

45 Shapley, L.S.: 'Cores of convex games', *International journal of game theory*, 1971, **1**, (1), pp. 11–26

46 Dwork, C., Roth, A., et al.: 'The algorithmic foundations of differential privacy', *Foundations and Trends® in Theoretical Computer Science*, 2014, **9**, (3–4), pp. 211–407

47 Littlechild, S.C., Owen, G.: 'A simple expression for the shapley value in a special case', *Management Science*, 1973, **20**, (3), pp. 370–372

48 'Mattugames: A game theoretical matlab toolbox to compute solution schemes and properties from tu-games'. `https://www.mathworks.com/matlabcentral/fileexchange/35933-mattugames`

49 Kullback, S., Leibler, R.A.: 'On information and sufficiency', *The annals of mathematical statistics*, 1951, **22**, (1), pp. 79–86