Quantum Game Analysis of Privacy-Leakage for Application Ecosystems

Shengling Wang
College of Information Science and Technology,
Beijing Normal University
Beijing, China
wangshengling@bnu.edu.cn

Jianhui Huang*
Institute of Computing Technology,
The Chinese Academy of Sciences
Beijing, China
huangjianhui@ict.ac.cn

Luyun Li
College of Information Science and Technology,
Beijing Normal University
Beijing, China
201521210001@mail.bnu.edu.cn

Liran Ma
Department of Computer Science,
Texas Christian University
Texas, USA
l.ma@tcu.edu

Xiuzhen Cheng
Department of Computer Science,
The George Washington University
Washington DC, USA
cheng@gwu.edu

ABSTRACT

Personalized applications often provide their functionality by extracting sensitive data from users. Such a strategy brings potential threats to users' privacy because malicious applications may sell users' sensitive data to third-parties for economic interests. The state-of-the-art literature addresses the privacy issue mainly from a technical perspective. In this paper, we take a different angle in which the main players involving privacy leakage are studied from a *connected* perspective rather than an *isolated* one. More specifically, we propose the concept of *application ecosystem*, which consists of user, application, and adversary (malicious third-party) as entities. Our aim is to analyze the tension forces inside the application ecosystem and their impacts on the behavior of each player, which can serve as a theoretical basis for designing effective and efficient privacy preservation solutions from a management level. Another outstanding trait of our analysis is the adoption of quantum game theory to model the application ecosystem, which is suitable because the important property of *entanglement* in quantum games can be employed to well depict the inner tension forces among the user, application, and adversary. This makes us take an important step towards understanding the complexity of decision-making from rational individuals. To the best of our knowledge, we are the first to quantize the privacy leakage issue. The simulation results quantitatively demonstrate how the mutual restrictions among all players determine their strategies and hence the development of the application ecosystem.

*Corresponding author

Mobihoc '17, Chennai, India

DOI: 10.1145/3084041.3084059

CCS CONCEPTS

•**Networks Network privacy and anonymity; Network privacy and anonymity; Security and privacy** *Formal methods and theory of security;*

ACM Reference format:
Shengling Wang, Jianhui Huang, Luyun Li, Liran Ma, and Xiuzhen Cheng. 2017. Quantum Game Analysis of Privacy-Leakage for Application Ecosystems. In *Proceedings of Mobihoc '17, Chennai, India, July 10-14, 2017,* 10 pages.
DOI: 10.1145/3084041.3084059

1 INTRODUCTION

A digital-savvy population is on the rise - many of us are constantly using various applications running on devices such as smartphones and fitness trackers. Most of these applications need to access user related information so as to provide intended functionalities. A typical example is the context-aware application where a user's private data such as geographical coordinates or activities are gathered to infer the user's contexts for providing personalized services.

Yet, such a personalized service may pose serious threats to users' privacy. The private information released to the applications is often attractive to third-parties such as digital marketers, which directly target an ever-increasing volume of customers. Subsequently, ill-intentioned applications, largely motivated by monetary incentives, intend to sell the private information to third-parties without users' consent. According to the statistics from [7], over 700 iOS applications surreptitiously leak the unique identity information of the devices, which may allow a third-party to construct a user' s preferences and usage patterns on applications. Furthermore, it has been revealed that 27 malware families (with 644 samples) are harvesting user accounts and text messages stored on the phones [25].

The growing threat of personal information leakage presses a need to develop countermeasures so as to protect individual privacy and security. The current mainstream solutions can be divided into two categories: i) analytical tools or systems aiming to detect and analyze malicious applications [3, 7, 8, 12, 23] to eliminate sources of privacy leakage; and ii) privacy control measures for different scenarios [11, 13, 16, 21] such as anonymizing sensitive data [13] or identities and selecting a suitable probability of releasing data

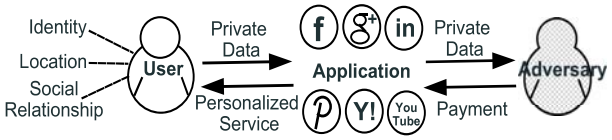


Figure 1: The application ecosystem.

for users [11, 16, 21]. These countermeasures typically address the privacy preservation problem purely from a technical perspective.

In this paper, we tackle the above issue from a different angle where the main entities involving privacy leakage are studied from a *connected* perspective rather than an *isolated* one. Our aim is to provide a theoretical basis for designing effective and efficient privacy preservation solutions from the management level. Compared to the existing approaches developed from a technical level, the management-based ones are usually simpler. For this purpose, we propose the concept of *application ecosystem* that includes three entities, i.e., user, application, and adversary (e.g., a malicious third-party). As shown in Fig. 1, in our proposed ecosystem, the user may need to give its private data to the application so as to obtain services, and the application may sell the data to the adversary for profits (e.g., monetary payments). Yet, the sale of the data, once discovered by the user, may lead to the distrust of the user on the application, and thus, the removal of the application from the user's device. As a result, the adversary has to conceal the identity of the application that leaks the user data; otherwise, the application may cease supplying data to the adversary.

The trust from the user on the application impacts the reputation of the application, while the concealment from the adversary on the application influences the reputation of the adversary. The reputation influential powers of the application and the adversary form two tension forces in our proposed application ecosystem, behaving like its *"light side"* and *"dark side"* because the former upholds its healthy development while the latter provides an asylum for privacy breaches and violations.

The existence of the *two sides of forces* enlightens us to address privacy leakage from a management level rather than a technical one. That is, after observing the power of the dark side, we can empower the light side by establishing a sound reputation mechanism for the application. Such a method obviously belongs to the scope of management, not that of the technical side. Naturally, we want to know whether or not this simple approach is effective. Hence, we need to answer the following question: *how do the powers of the two sides impact the behaviors of the three entities in an application ecosystem?* In other words, under the two influential powers of reputation, to what extent is the user willing to release private data, the application inclined to sell the data, and the adversary consenting to provide an umbrella to malicious applications?

The answer to the aforementioned question can offer a straightforward explanation on how to quantitatively determine the reputation influential power of the application to resist that of the adversary in order to make the application ecosystem sustainable and healthy. To find an answer, we adopt game theory to analyze the application ecosystem. This is because the inner tension forces between the user and the application as well as that between the application and the adversary stem from their cooperative and conflicting relationships, while game theory provides efficient tools to deal with such corporations and contradictions.

A salient feature of our study is the adoption of quantum games that extend the classical ones to the quantum domain based on quantum information theory. Many instances [5, 14] demonstrate that quantum games outperform classical ones, resulting in their wide applications [4, 10, 19]. The advantage of a quantum game mainly originates from the extended strategy space and the concept of *entanglement*. The former allows the optimal strategy to be found from a wider range, and the latter offers another perspective to depict the relationship among rational individuals. Quantum games are suitable for analyzing an application ecosystem because the inner tension forces among the user, the application, and the adversary can be well depicted by their entanglement. Since the *entanglement* (the inner tension forces) can affect the strategy of each player in a quantum game, which cannot be reflected by classical games, we take an important step towards understanding the complexity of decision-making from rational individuals using quantum games.

To the best of our knowledge, we are the first to quantize the privacy leakage issue, using quantum game model to study the behavior of each player under the impact of inner tension forces in the application ecosystem. Conclusively, our contributions can be summarized as follows:

- An application ecosystem is formulated by a quantum game model, which has the entangled inputs taking advantage of two entanglement degrees to depict the power of the light side and that of the dark side (i.e., the reputation influential powers of the application and the adversary).
- The relationship between the optimal strategies of the players and their entanglement is deduced, through which one can quantitatively analyze how the reputation influential powers of the application and the adversary impact the development of the application ecosystem.
- Two special cases are also analyzed. As supplements, such analyses make our study for privacy leakage in the application ecosystem complete.

The remainder of the paper is organized as follows. A summary of related work is presented in Section 2. Section 3 offers a brief introduction to quantum game theory while the utility model and the quantum game model for the application ecosystem are respectively presented in Sections 4 and 5. The method for deriving the best strategy for each player is given in Section 6. Section 7 analyzes two special cases that may happen in an application ecosystem. Section 8 reports the results of our numerical simulations. Finally, our conclusions are summarized in Section 9.

2 RELATED WORK

As privacy-leaking applications are becoming commonplace, there is a pressing need to develop countermeasures. As a result, a number of solutions such as *TaintDroid* [8], *AdRisk* [12], and *PiOS* [7] were proposed to detect such applications. *TaintDroid* [8] is a taint tracking and analytical tool that can track multiple sources of private data concurrently. *AdRisk* [12] is a system that can identify

100 representative in-app ad libraries from 100,000 popular Android applications; such in-app ad libraries can impose the risks of releasing sensitive data and executing untrusted programs. *PiOS* [7] is a tool for analyzing privacy leakage in Apple's iOS system via creating a control flow graph for applications.

Different from those works focusing on the discovery of sensitive data release, [3] and [23] tackle the fuzzy nature of the privacy leakage detection problem. To determine whether a sensitive information delivery serves for intended functions of the application itself or others, *DroidJust* [3] was proposed; to evaluate whether the transmission of sensitive data is user-intended, *AppIntent* [23] was developed. *AppIntent* provides a sequence of operations with each corresponding to a data transmission event to help an analyst figure out whether a transmission is legal.

Another line of mainstream work in countering privacy leak focuses on privacy control [11, 13, 16, 21]. Hornyack *et al.* [13] retrofitted the Android operating system to implement two privacy control measures, i.e., replacing private data with shadow ones and blocking the transmission of the data that are only allowed for on-device use, without modifying the applications. Additionally, [11, 16, 21] target privacy preservation for context-aware mobile applications. *MaskIt* [11] is a middleware that limits what an adversary can learn by filtering a user's sensitive context stream. This work assumes that an adversary adopts static strategies. To address this deficiency, [21] formulates the competition between users and adversaries as a zero-sum stochastic game and proposes a minimax learning algorithm to compute the optimal defense strategy. Nevertheless, the importance of the applications' strategies was ignored by [11, 21]. Hence, Li *et al.* [16] employed an extensive form game to formulate the decision-making process of the users, applications, and adversaries, and obtained its Nash equilibrium.

In summary, the state-of-the-art countermeasures preserve privacy from a technical point of view, focusing on either analyzing/detecting malicious applications or implementing various privacy controls for different scenarios.

3 INTRODUCTION OF QUANTUM GAME

Quantum game is an important development in quantum computing. The two pioneer work [5] and [14] on quantum games respectively study the following two classical problems: the *penny flip* problem and the *prisoner's dilemma* problem. Meyer [5] proved that a quantum player can always beat his classical opponent in the *penny flip* problem. Eisert *et al.* [14] employed a quantum game to formulate the *prisoner's dilemma*, and found a new Nash equilibrium that can maximize the social welfare in certain cases. This implies that the dilemma in quantum game may not exist under certain conditions.

Following these pioneer work, the superiority of quantum games was investigated in more depth. Quantum game theory has been applied to economics [19], biology [10], and computer science [4]. The superior power of quantum games mainly stems from the extended strategy space and the concept of *entanglement*. More specifically, with an extended strategy space, namely the *Hilbert* space, an optimal strategy can be searched from a wider range. The idea of entanglement offers another perspective to depict the relationship among rational individuals, which is especially important since the relationship is critical for determining a player's strategy. Therefore, taking advantage of the superior power of quantum games, one can better understand the complexity of decision-making from rational individuals.

Quantum games are based on quantum mechanics and quantum information theory. In quantum mechanics, a physical system is associated with a state space, the *Hilbert* space. A state can be represented by *bit(s)* in classical information theory, where a bit usually has definite values of 0 or 1. Similarly, a state in a Hilbert space can be expressed by *a quantum bit* (or *qubit*). A qubit often has two possible values: $|0\rangle$ and $|1\rangle$, where $|\cdot\rangle$ is the Dirac symbol. A qubit can also be the linear combination of the basic states $|0\rangle$ and $|1\rangle$. For example $a|0\rangle+b|1\rangle$ defines a state indicating that the system behaves like $|0\rangle$ with probability $|a|^2$ and like $|1\rangle$ with probability $|b|^2$ [2].

If a composite physical system consists of multiple sub-systems, e.g., $s_1, s_2, \cdots, s_n$, then its state is the tensor product of all sub-systems' states, namely $\rho_1 \otimes \rho_2 \cdots \otimes \rho_n$, where ρ_i is the state of sub-system s_i and $\otimes$ is the notation of tensor product.

In certain scenarios, the state of a composite physical system cannot be represented as the tensor product of all sub-systems' states; instead, it appears in a fashion of an entangled state, which means that the sub-systems interact in ways such that the quantum state of each sub-system cannot be described independently.

In the following, we will employ quantum game theory to analyze our application ecosystem.

4 EXPECTED UTILITY OF EACH PLAYER

Because the strategy of a rational player in an application ecosystem is often utility motivated, we shed light on the utility of each player in advance. The utility of a player is affected by the subtle connections among the user, the application, and the adversary. Specifically, the user needs to decide whether or not to release private information to the application: the release of such information may gain personalized services, but jeopardize user privacy; the application needs to make a decision on whether to sell the user's personal data to the adversary: the sale of the user data may produce profits for the application, but harm the reputation of the application; the adversary needs to find a balance between maintaining a good trust with the application and reducing the cost of realizing such an aim: exploiting the user's data may reveal the malicious behavior of the application, leading to the mistrust between the application and the adversary; this mistrust can cause the application to cease supplying data to the adversary, forcing the adversary to perform further data processing so as to conceal the identity of the application, which obviously incurs cost to the adversary.

We give an example to illustrate the connections among the utilities of the three players. In location-based services (LBS), a user needs to report its location to the server who may sell this information to an adversary (e.g. a location-based advertiser) for better utility. However, once the malicious behavior is exposed, the user may offload the LBS application, making the adversary lose the data provider. Hence, the location-based advertiser may obfuscate the location information when it uses the personal data, lowering the chance of exposing the LBS application because the

user does not know whether the location information was disclosed due to the LBS application or other applications used in adjacent places. Undoubtedly, location obfuscation increases the cost of the location-based advertiser, thus decreasing its utility.

According to the above analysis, the expected utility (U_u) of an application requiring a user's personal data d can be formulated as

$$U_u = q_u Q - k s_d q_u q_p, \tag{1}$$

where the first part is the profit ($Q > 0$) obtained from the service if the user releases its data and the second part refers to the equivalent monetary loss due to privacy leak; and q_u and q_p are respectively the probabilities of the user and the application to release and leak the private information. Note that the loss resulted from privacy leakage is proportional to the sensitivity of information d, denoted by $s_d \in [0, 1]$, and $k > 0$ is the corresponding proportional coefficient; also note that s_d can be calculated using a similar approach as the one in *MaskIt* [11].

The expected utility U_d of the adversary, as shown in (2), involves i) the profit $p(s_d)$ obtained from exploiting the private data, which is related to the information sensitivity s_d; ii) the financially equivalent reputation loss $\alpha(q_d)\theta$, where $\alpha(q_d)$ is the reputation loss of the adversary related to the extent ($q_d \in [0, 1]$) at which the identity of the application is exposed by the adversary, and θ (> 0) is the reputation loss impactor (i.e. the reputation influential power) that is usually controlled by some management rules negotiated between the application and the adversary; and iii) the cost of concealing the identity of the application $c(1 - q_d)$, which is directly proportional to q_d (with a negative proportionality constant) and c (> 0) is the corresponding coefficient.

$$U_d = \Big(p(s_d) - \alpha(q_d)\theta - c(1 - q_d)\Big) q_u q_p. \tag{2}$$

In (2), $\alpha(q_d)$ can be modeled by a Sigmoid function [20] as shown in (3), which is often employed to depict a person's subjective feeling on some objective situation, such as the received quality of service, where q_0 (> 0) is the identity exposition level leading to a basic reputation loss from the application, below which the reputation loss is limited (convex segment) and above which the reputation loss quickly approaches to an asymptotic value (concave segment). The steepness of the satisfactory curve is decided by ϵ (> 0).

$$\alpha(q_d) = \frac{1}{1 + e^{-\epsilon(q_d - q_0)}}. \tag{3}$$

The expected utility (U_p) of the application involves the revenue ($R > 0$) from providing a service and the profit ($m(s_d) > 0$) from leaking private data d that is related to the private information sensitivity s_d, as well as the monetarily equivalent reputation loss due to privacy leakage:

$$U_p = q_u R + \Big(m(s_d) - \beta(q_d)\phi\Big) q_u q_p. \tag{4}$$

Here ϕ is the reputation loss impactor (i.e. the reputation influential power) of the application, reflecting how the reputation loss impacts its utility, and can be determined by some management mechanism posed on the application to regulate its behavior; $\beta(q_d)$ (> 0) is the reputation loss which depends on the extent (q_d) at which the application is exposed and can also be modeled by a Sigmoid function, i.e., $\beta(q_d) = \frac{1}{1+e^{-\nu(q_d - \omega_0)}}$, where ν (> 0) and ω_0 (> 0) are the parameters whose functions are similar to ϵ and q_0 in (3), respectively.

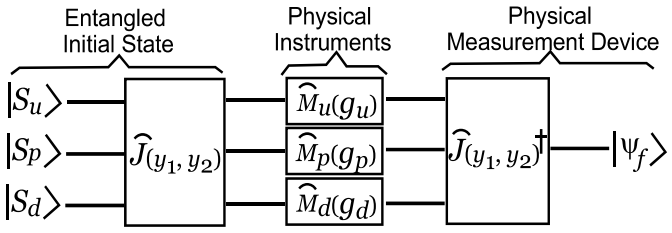


Figure 2: The quantum model.

Obviously, ϕ and θ, respectively representing the reputation influential powers of the application and the adversary, are the *"light side"* and the *"dark side"* in the application ecosystem, respectively. The larger ϕ and the smaller θ, the healthier the ecosystem and vice visa.

5 QUANTUM MODEL FOR THE APPLICATION ECOSYSTEM

To model an application ecosystem, the strategy space of each player needs to be carefully defined. Specifically, if the user is willing to release private data to the application, it is in the cooperation state $|C\rangle$; otherwise, the user is in the defection state $|D\rangle$. The cooperation state $|C\rangle$ of the application is defined as keeping the user's private data confidential, and the defection state $|D\rangle$ refers to the state of releasing the user data to the adversary. The adversary is considered to be in the cooperation state $|C\rangle$ if it exposes the identity of the application when using data, and otherwise, it is regarded as in the defection state $|D\rangle$. Based on these definitions, the initial state of each player, i.e., $|S_u\rangle$, $|S_p\rangle$, and $|S_d\rangle$ can be any of the basic states, namely $|C\rangle$ or $|D\rangle$, or the linear combinations of them.

To analyze the application ecosystem, a popular quantum model [1, 14, 15] shown in Fig. 2 is employed, which is consisted of the following three components:

- an entangled initial state formed by entangling the tensor product of each player's initial state;
- a set of physical instruments that make each player capable of controlling its qubit according to some strategy;
- a physical measurement device evaluating the payoff of each player according to the state of each player.

This model starts from the state $|S_u\rangle \otimes |S_p\rangle \otimes |S_d\rangle$, which is the tensor product of the initial states of the user, the application, and the adversary. After that, the state $|S_u\rangle \otimes |S_p\rangle \otimes |S_d\rangle$ is entangled by an exoteric unitary operator J. Consequently, an entangled initial state $|\psi_i\rangle = J(|S_u\rangle \otimes |S_p\rangle \otimes |S_d\rangle)$ is formed, from which the competition among the players in the application ecosystem begins. The strategies of the user, the application, and the adversary are determined by a set of physical instruments, namely the unitary operators M_u, M_p, and M_d, respectively. After executing the moves, each player transmits its qubit to the measurement device to evaluate the final payoff. However, to ensure that the classical game remains embedded within the quantum one [15], the measurement device needs to contain a disentangling gate $J^\dagger$, where $JJ^\dagger = 1$, which means that J is a *unitary operator*. As a result, the final state

$|\psi_f\rangle$ of the quantum model is:

$$|\psi_f\rangle = J^\dagger(M_u \otimes M_p \otimes M_d)J(|S_u\rangle \otimes |S_p\rangle \otimes |S_d\rangle). \quad (5)$$

In (5), for conciseness, the entanglement operator J is selected as follows, which is similar to that in [15]:

$$J = \exp\{iy_1 x_u p_p + iy_2 x_p p_d\}, \quad (6)$$

where y_1 and y_2 represent the entanglement degrees between the user and the application, and the application and the adversary, respectively. In our study, $y_1 = \phi$ and $y_2 = \theta$. This indicates that the entanglement between the user and the application as well as that between the application and the adversary mainly depends on their reputation influential powers.

In (6), the position operators of the user and the application, namely $x_u = (a_u^\dagger + a_u)/\sqrt{2}$ and $x_p = (a_p^\dagger + a_p)/\sqrt{2}$, are observable variables that can be measured eventually; and the momentum operators of the application and the adversary are $p_p = i(a_p^\dagger - a_p)/\sqrt{2}$ and $p_d = i(a_d^\dagger - a_d)/\sqrt{2}$, respectively. Note that here $a_u^\dagger$, $a_p^\dagger$, and $a_d^\dagger$ are respectively the creation operators of the user, the application, and the adversary, and a_u, a_p, and a_d are respectively the corresponding annihilation operators. Therefore, we have

$$J = \exp\{-y_1(a_u^\dagger a_p^\dagger - a_u a_p) - y_2(a_p^\dagger a_d^\dagger - a_p a_d)\}.$$

Since the user only interacts with the application and the adversary only trades with the application in an application ecosystem, the position operator of the user x_u is only entangled with the momentum operator of the application p_p; the same situation happens for the position operator of the application x_p and the momentum operator of the adversary p_d in the entanglement operator J, where the communication between the position operator and the momentum operator of one player is ignored.

As in [15], the following strategy form is adopted in this paper:

$$M_i = \exp\{-ig_i p_i\},\ g_i \in [0, \infty),\ i \in \{u, p, d\},$$

where g_u, g_p, and g_d are the strategy parameters of the user, the application, and the adversary, respectively.

6 SOLUTIONS FOR OPTIMAL STRATEGIES

After establishing the quantum model for the application ecosystem, we can now determine the optimal strategies for all players, i.e. q_u^*, q_p^*, and q_d^*. Our derivation learns from [24]. Because $JJ^\dagger = 1$, we have $J^\dagger = \exp\{y_1(a_u^\dagger a_p^\dagger - a_u a_p) + y_2(a_p^\dagger a_d^\dagger - a_p a_d)\}$. Taking advantage of the Baker-Campbell-Hausdorff formula [9], we obtain:

$$J^\dagger a_u J = \sum_{n=0}^{\infty} \frac{1}{n!}[[y_1(a_u^\dagger a_p^\dagger - a_u a_p) + y_2(a_p^\dagger a_d^\dagger - a_p a_d)]^{(n)}, a_u]$$

$$= a_u - y_1 a_p^\dagger + \frac{y_1^2 a_u + y_1 y_2 a_d}{2!} - \frac{y_1(y_1^2 + y_2^2)a_p^\dagger}{3!} +$$

$$\frac{y_1^2(y_1^2 + y_2^2)a_u + y_1 y_2(y_1^2 + y_2^2)a_d}{4!} - \frac{y_1(y_1^2 + y_2^2)^2 a_p^\dagger}{5!} +$$

$$\frac{y_1^2(y_1^2 + y_2^2)^2 a_u + y_1 y_2(y_1^2 + y_2^2)^2 a_d}{6!} - \frac{y_1(y_1^2 + y_2^2)^3 a_p^\dagger}{7!}$$

$$+ \ldots + [[y_1(a_u^\dagger a_p^\dagger - a_u a_p) + y_2(a_p^\dagger a_d^\dagger - a_p a_d)]^n, a_u],$$

where $[x, y]$ is the commutator of x and y. We will detail the calculation of $J^\dagger a_u J$ in the appendix. By employing a similar method, we can calculate $J^\dagger a_u^\dagger J$. Because $p_u = i(a_u^\dagger - a_u)/\sqrt{2}$, we have

$$J^\dagger p_u J = J^\dagger \frac{i}{\sqrt{2}}(a_u^\dagger - a_u)J = \frac{i}{\sqrt{2}}(J^\dagger a_u^\dagger J - J^\dagger a_u J)$$

$$= p_u\Big(1 + \frac{y_1^2}{2!} + \frac{y_1^2}{4!}(y_1^2 + y_2^2) + \frac{y_1^2}{6!}(y_1^2 + y_2^2)^2 +$$

$$\ldots + \frac{y_1^2}{(2n+2)!}(y_1^2 + y_2^2)^n\Big) + p_p\Big(y_1 + \frac{y_1}{3!}(y_1^2 + y_2^2) +$$

$$\frac{y_1}{5!}(y_1^2 + y_2^2)^2 + \frac{y_1}{7!}(y_1^2 + y_2^2)^3 + \ldots + \frac{y_1}{(2n+1)!}(y_1^2 + y_2^2)^n\Big)$$

$$+ p_d\Big(\frac{y_1 y_2}{2!} + \frac{y_1 y_2}{4!}(y_1^2 + y_2^2) + \frac{y_1 y_2}{6!}(y_1^2 + y_2^2)^2$$

$$+ \ldots + \frac{y_1 y_2}{(2n+2)!}(y_1^2 + y_2^2)^n\Big)$$

$$= p_u\Big(1 + \sum_{n=0}^{\infty} \frac{y_1^2}{(2n+2)!}(y_1^2 + y_2^2)^n\Big) +$$

$$p_p \sum_{n=0}^{\infty} \frac{y_1}{(2n+1)!}(y_1^2 + y_2^2)^n + p_d \sum_{n=0}^{\infty} \frac{y_1 y_2}{(2n+2)!}(y_1^2 + y_2^2)^n.$$

Similarly, we can get

$$J^\dagger p_p J = p_u \sum_{n=0}^{\infty} \frac{y_1}{(2n+1)!}(y_1^2 + y_2^2)^n +$$

$$p_p \sum_{n=0}^{\infty} \frac{1}{(2n)!}(y_1^2 + y_2^2)^n + p_d \sum_{n=0}^{\infty} \frac{y_2}{(2n+1)!}(y_1^2 + y_2^2)^n$$

and

$$J^\dagger p_d J = p_u \sum_{n=0}^{\infty} \frac{y_1 y_2}{(2n+2)!}(y_1^2 + y_2^2)^n + p_p \sum_{n=0}^{\infty}$$

$$\frac{1}{(2n+1)!}(y_1^2 + y_2^2)^n + p_d\Big(1 + \sum_{n=0}^{\infty} \frac{y_2^2}{(2n+2)!}(y_1^2 + y_2^2)^n\Big).$$

Therefore,

$$J^\dagger M_u J = J^\dagger \exp\{-ig_u p_u\}J = J^\dagger \frac{1}{n!}\sum_{n=0}^{\infty}(-ig_u p_u)^n J$$

$$= \frac{1}{n!}\sum_{n=0}^{\infty}(-ig_u)^n (J^\dagger p_u J)^n = \exp\{-ig_u J^\dagger p_u J\}$$

$$= \exp\{-ig_u\Big(p_u\Big(1 + \sum_{n=0}^{\infty}\frac{y_1^2(y_1^2 + y_2^2)^n}{(2n+2)!}\Big) +$$

$$p_p \sum_{n=0}^{\infty}\frac{y_1(y_1^2 + y_2^2)^n}{(2n+1)!} + p_d \sum_{n=0}^{\infty}\frac{y_1 y_2(y_1^2 + y_2^2)^n}{(2n+2)!}\Big)\}.$$

Taking a similar method, we obtain the following results:

$$J^\dagger M_p J = \exp\{-ig_p\Big(p_u \sum_{n=0}^{\infty}\frac{y_1(y_1^2 + y_2^2)^n}{(2n+1)!} +$$

$$p_p \sum_{n=0}^{\infty}\frac{(y_1^2 + y_2^2)^n}{(2n)!} + p_d \sum_{n=0}^{\infty}\frac{y_2(y_1^2 + y_2^2)^n}{(2n+1)!}\Big)\}$$

and

$$J^{\dagger}M_dJ = \exp\{-ig_d\Big(p_u\sum_{n=0}^{\infty}\frac{y_1y_2(y_1^2+y_2^2)^n}{(2n+2)!} + p_p\sum_{n=0}^{\infty}\frac{y_2(y_1^2+y_2^2)^n}{(2n+1)!} + p_d\Big(1+\sum_{n=0}^{\infty}\frac{y_2^2(y_1^2+y_2^2)^n}{(2n+2)!}\Big)\Big)\}.$$

In light of (5), the final state $|\psi_f\rangle$ of the quantum model can be reformed as:

$$\begin{aligned}|\psi_f\rangle =& \Big(J^{\dagger}M_uJ\Big)\otimes\Big(J^{\dagger}M_pJ\Big)\otimes\Big(J^{\dagger}M_dJ\Big)\otimes|S_u\rangle\otimes|S_p\rangle\otimes|S_d\rangle\\ =& \exp\{-\Big(g_u(1+\sum_{n=0}^{\infty}\frac{y_1^2(y_1^2+y_2^2)^n}{(2n+2)!}) + g_p\sum_{n=0}^{\infty}\frac{y_1(y_1^2+y_2^2)^n}{(2n+1)!}\\ &+g_d\sum_{n=0}^{\infty}\frac{y_1y_2(y_1^2+y_2^2)^n}{(2n+2)!}\Big)ip_u\}\otimes|S_u\rangle\otimes\exp\{-\Big(g_u\sum_{n=0}^{\infty}\\ &\frac{y_1(y_1^2+y_2^2)^n}{(2n+1)!} + g_p\sum_{n=0}^{\infty}\frac{(y_1^2+y_2^2)^n}{(2n)!} + g_d\sum_{n=0}^{\infty}\frac{y_2(y_1^2+y_2^2)^n}{(2n+1)!}\Big)\\ &ip_p\}\otimes|S_p\rangle\otimes\exp\{-\Big(g_u\sum_{n=0}^{\infty}\frac{y_1y_2(y_1^2+y_2^2)^n}{(2n+2)!} + g_p\\ &\sum_{n=0}^{\infty}\frac{y_1(y_1^2+y_2^2)^n}{(2n+1)!} + g_d(1+\sum_{n=0}^{\infty}\frac{y_2^2(y_1^2+y_2^2)^n}{(2n+2)!})\Big)ip_d\}\otimes|S_d\rangle.\end{aligned}$$

Thus, q_u, q_p, and q_d, according to the quantum model, can be calculated as:

$$\begin{aligned}q_u =& g_u(1+\sum_{n=0}^{\infty}\frac{y_1^2(y_1^2+y_2^2)^n}{(2n+2)!}) + g_p\sum_{n=0}^{\infty}\frac{y_1(y_1^2+y_2^2)^n}{(2n+1)!} +\\ & g_d\sum_{n=0}^{\infty}\frac{y_1y_2(y_1^2+y_2^2)^n}{(2n+2)!},\end{aligned}$$

$$\begin{aligned}q_p =& g_u\sum_{n=0}^{\infty}\frac{y_1(y_1^2+y_2^2)^n}{(2n+1)!} + g_p\sum_{n=0}^{\infty}\frac{(y_1^2+y_2^2)^n}{(2n)!}\\ &+g_d\sum_{n=0}^{\infty}\frac{y_2(y_1^2+y_2^2)^n}{(2n+1)!}\end{aligned}$$

and

$$\begin{aligned}q_d =& g_u\sum_{n=0}^{\infty}\frac{y_1y_2(y_1^2+y_2^2)^n}{(2n+2)!} + g_p\sum_{n=0}^{\infty}\frac{y_1(y_1^2+y_2^2)^n}{(2n+1)!}\\ &+g_d(1+\sum_{n=0}^{\infty}\frac{y_2^2(y_1^2+y_2^2)^n}{(2n+2)!}\Big).\end{aligned}$$

Note that q_u, q_p, and q_d are the outputs (measurement results) of the quantum model. All that a player can control is its strategy parameters, namely, g_u, g_p, and g_d. To find the optimal strategy for each player, the optimal strategy parameters g_u^*, g_p^*, and g_d^* should be determined by maximizing U_u, U_p, and U_d with the constraints of $0 \le q_u, q_p, q_d \le 1$. This is a multi-objective and multi-constraint problem. Due to its high complexity and non-linearity, we adopt a multi-objective evolutionary algorithm to search for the Pareto optimal solutions [6]. The description of the algorithm is omitted, and interested readers are referred to [6] for details.

Note that in this study, we intend to obtain the Pareto optimal solutions rather than the Nash Equilibriums because the former are the optimal results when the global information is obtained while the latter are the local optimal ones when the information is asymmetric. Our research aims to establish a sound reputation mechanism for the application according to the utilities of the three players observed by a manager, addressing the privacy leakage issue in application ecosystems from a management level. Hence, the manager with the global information has the capacity to obtain the Pareto optimal solutions rather than the Nash Equilibriums.

7 SPECIAL CASES

In this section, we analyze two special cases appeared in typical application ecosystems. In both cases, the best strategy of the adversary is not to hide the identity of the application.

7.1 The Malicious Application Would Expose Itself in Any Condition

In some scenarios, once an application leaks a user's private data to an adversary, its identity must be exposed no matter how the adversary behaves. For example, in the cases when the speciality of an application makes it the only sensitive data provider or the user tells its private information only to one application, the user obviously can infer which application is malicious. In such scenarios, the best strategy of the adversary is not to conceal the identity of the application to save the cost of dealing with the data. That is $q_d^* = 1$. This deterministic strategy makes only two players remain in the application ecosystem, namely the user and the application. Moreover, the expected utility of the user remains unchanged while that of the application changes to $q_uR + \Big(m(s_d) - \beta(1)\phi\Big)q_uq_p$.

To analyze the strategies of the user and the application, we again employ a quantum game to formulate the application ecosystem, where a quantum model similar to that shown in Fig. 2 is adopted and the derivation of the optimal strategies is also learned from [24]. This model begins with the tensor product of the initial states of the user and the application, i.e. $|S_u\rangle \otimes |S_p\rangle$. After applying entanglement based on an exoteric unitary operator U, we obtain the entangled initial state $|\varphi_i\rangle = U(|S_u\rangle \otimes |S_p\rangle)$. The user and the application respectively execute their moves on the entangled initial state through the unitary operators, i.e., M_u and M_p, determined by a set of physical instruments. Then the results pass through a disentangling gate $U^{\dagger}$ before they are sent to the measurement device for evaluating the payoff of each player. Finally, the output of the quantum model, i.e. the following final state $|\varphi_f\rangle$ is obtained:

$$\begin{aligned}|\varphi_f\rangle &= U^{\dagger}(M_u\otimes M_p)U(|S_u\rangle\otimes|S_p\rangle)\\ &= \Big(U^{\dagger}M_uU\Big)\otimes\Big(U^{\dagger}M_pU\Big)\otimes|S_u\rangle\otimes|S_p\rangle,\end{aligned}$$

where the entanglement operator U has the following form:

$$U = \exp\{iy_1x_up_p\}. \tag{7}$$

Because there are only two players in this application ecosystem, the entanglement operator U involves only one entanglement degree, namely y_1. We let $y_1 = \phi$, implying that the entanglement between the user and the application is the reputation influential power of the application, which represents the trust between them.

In (7), $x_u = (a_u^\dagger + a_u)/\sqrt{2}$ and $p_p = i(a_p^\dagger - a_p)/\sqrt{2}$, and hence

$$U = \exp\{-y_1(a_u^\dagger a_p^\dagger - a_u a_p)\}.$$

To find the optimal strategies for the user and the application, we need to analyze (7), where $U^\dagger M_u U$ and $U^\dagger M_p U$ should be solved in advance. In fact, because $M_u = \exp\{-ig_u p_u\}$ $g_u \in [0, \infty)$, and $p_u = i(a_u^\dagger - a_u)/\sqrt{2}$, we have

$$U^\dagger M_u U = U^\dagger \exp\{-ig_u p_u\} U = U^\dagger \frac{1}{n!} \sum_{n=0}^{\infty} (-ig_u p_u)^n U \tag{8}$$

$$= \frac{1}{n!} \sum_{n=0}^{\infty} (-ig_u)^n (U^\dagger p_u U)^n = \exp\{-ig_u U^\dagger p_u U\},$$

where

$$U^\dagger p_u U = U^\dagger \frac{i}{\sqrt{2}}(a_u^\dagger - a_u) U = \frac{i}{\sqrt{2}}(U^\dagger a_u^\dagger U - U^\dagger a_u U) \tag{9}$$

$$= p_u \sum_{n=0}^{\infty} \frac{1}{(2n)!} y_1^{2n} + p_p \sum_{n=0}^{\infty} \frac{1}{(2n+1)!} y_1^{2n+1}$$

$$= p_u \frac{e^{y_1} + e^{-y_1}}{2} + p_p \frac{e^{y_1} - e^{-y_1}}{2}.$$

The result of (9) stems from

$$U^\dagger a_u^\dagger U = \sum_{n=0}^{\infty} \frac{1}{n!} [[y_1(a_u^\dagger a_p^\dagger - a_u a_p)]^{(n)}, a_u] \tag{10}$$

$$= a_u^\dagger \sum_{n=0}^{\infty} \frac{1}{(2n)!} y_1^{2n} - a_p \sum_{n=0}^{\infty} \frac{1}{(2n+1)!} y_1^{2n+1}$$

and

$$U^\dagger a_u U = \sum_{n=0}^{\infty} \frac{1}{n!} [[y_1(a_u^\dagger a_p^\dagger - a_u a_p)]^{(n)}, a_u] \tag{11}$$

$$= a_u \sum_{n=0}^{\infty} \frac{1}{(2n)!} y_1^{2n} - a_p^\dagger \sum_{n=0}^{\infty} \frac{1}{(2n+1)!} y_1^{2n+1}.$$

Both (10) and (11) can be solved based on a similar approach as the one introduced in the appendix.

Plugging (9) into (8), we have

$$U^\dagger M_u U = \exp\{-ig_u \big(p_u \frac{e^{y_1} + e^{-y_1}}{2} + p_p \frac{e^{y_1} - e^{-y_1}}{2}\big)\}. \tag{12}$$

Employing a similar method, we obtain:

$$U^\dagger M_p U = \exp\{-ig_p \big(-p_u \frac{e^{y_1} - e^{-y_1}}{2} + p_p \frac{e^{y_1} + e^{-y_1}}{2}\big)\}. \tag{13}$$

Plugging (12) and (13) into (7), we get the final $|\varphi_f\rangle$ as follows:

$$|\varphi_f\rangle = \exp\{-ip_u \big(g_u \frac{e^{y_1} + e^{-y_1}}{2} - g_p \frac{e^{y_1} - e^{-y_1}}{2}\big)\} \otimes |S_u\rangle \otimes$$
$$\exp\{-ip_p \big(g_u \frac{e^{y_1} - e^{-y_1}}{2} + g_p \frac{e^{y_1} + e^{-y_1}}{2}\big)\} \otimes |S_p\rangle.$$

Thus, the strategies of the user and the application, i.e., q_u and q_p, can be calculated as

$$q_u = g_u \frac{e^{y_1} + e^{-y_1}}{2} - g_p \frac{e^{y_1} - e^{-y_1}}{2}, \tag{14}$$

$$q_p = g_u \frac{e^{y_1} - e^{-y_1}}{2} + g_p \frac{e^{y_1} + e^{-y_1}}{2}. \tag{15}$$

Based on (14) and (15), we can determine the best strategy for each player by finding the best strategy parameters, g_u^* and g_p^*, which are also the controllable parameters of the players in the quantum game model. Note that g_u^* and g_p^* should maximize the utilities of both players while guaranteeing $0 \le q_u$ and $q_p \le 1$. The problem of finding g_u^* and g_p^* is obviously a multi-objective and multi-constraint one. Hence, we employ the multi-objective evolutionary algorithm used in Section 6 to search for the Pareto optimal solutions.

7.2 The Malicious Application is Hardly Detected

Another special case under our consideration is when an application releases the private data which is hardly detected. For example, if the application sells the user's ID to the adversary but the ID actually can be obtained from multiple sources, implying the user can hardly tell which application is the real betrayer. In this scenario, the best strategy for the adversary is not to process the private data to reduce the related cost. As the application does not have the reputation loss even though it behaves maliciously, its expected utility turns into $q_u R + m(s_d) q_u q_p$. In this case, the best strategy of the application to maximize the expected utility is definitely to disclose the private data, i.e. $q_p^* = 1$. For the user, its strategy depends on its expected utility, i.e., $U_u = q_u(Q - ks_d)$. Obviously, $q_u = 1$ if $Q > ks_d$ and otherwise $q_u = 0$.

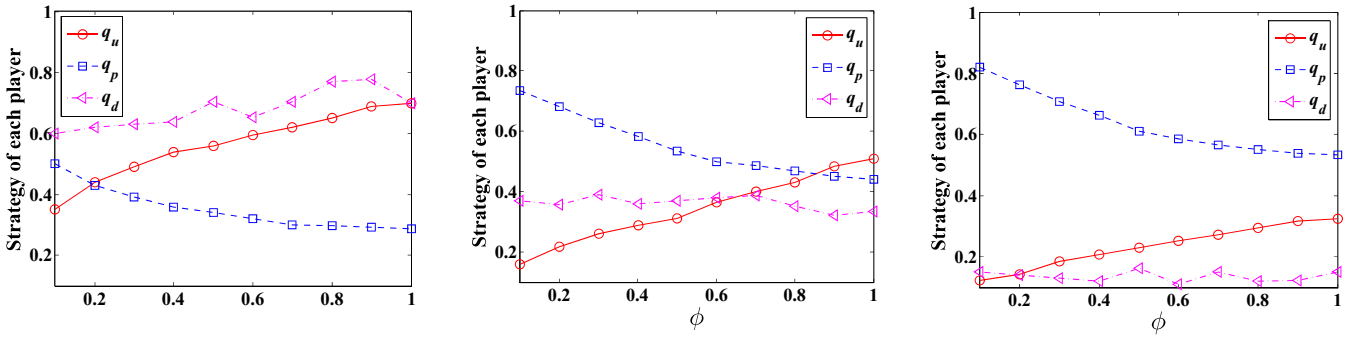
From the above analysis, one can see that the privacy issue is hard to tackle by developing a reputation mechanism for applications in this special case. That is, the solutions from the management level may not work and the existing approaches from the technical level, such as those proposed for malicious application detection [7, 8, 12] or privacy control [11, 13, 16–18, 21, 22], may be the best to tackle the challenges of privacy leak in this case.

8 NUMERICAL ANALYSIS

We present our numerical analysis results in this section to demonstrate how the reputation influential powers of the application and the adversary affect the strategies of the three elements in an application ecosystem in the general case and the first special case presented in Section 7. Note that extensive simulations have been performed but only some of the results are reported due to the similar change trends.

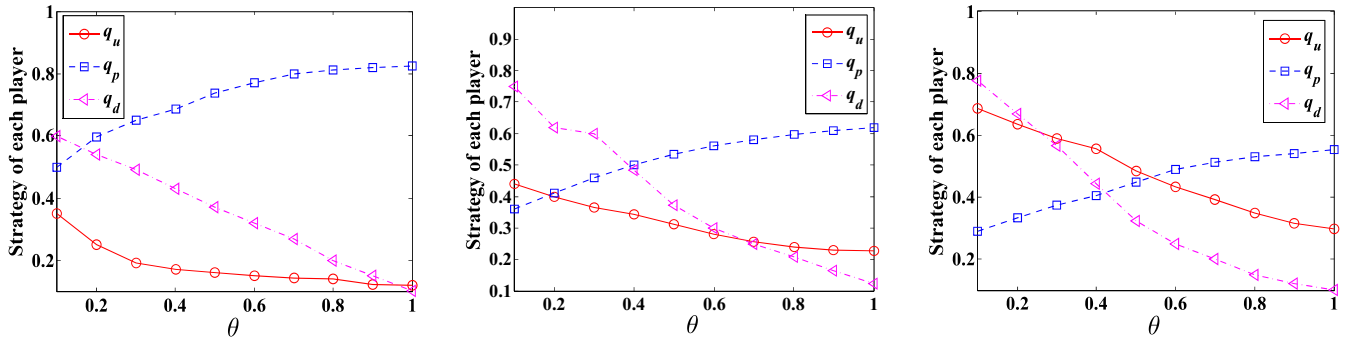
To simulate the performance in the general case, we fix $Q = 1.5$, $s_d = 0.5$, $c = 0.9$, $R = 2$, $k = 15$, and set $p(s_d)$ and $m(s_d)$ to be linear functions with the coefficients of 1.5 and 1, respectively. The parameters in the two Sigmod functions $\alpha(s_d)$ and $\beta(s_d)$ are set as follows: $\epsilon = \nu = 1$ and $q_0 = \omega_0 = 0$.

Figs. 3 (a) (b) (c) illustrate how the strategies of the three players change with the reputation influential power of the application, i.e. ϕ, when $\theta = 0.1, 0.5$, and 0.9, respectively. All subfigures demonstrate one common trend: with the increase of ϕ, q_p goes down, q_u rises up, while fluctuation happens on q_d. The reason behind this phenomena is that when ϕ increases, the reputation influential power of the application raises, making the application care more about the evaluation from the user and thus it would



(a) $\theta = 0.1$ (b) $\theta = 0.5$ (c) $\theta = 0.9$

Figure 3: How the strategies of three players change with the reputation influential power of the application.



(a) $\phi = 0.1$ (b) $\phi = 0.5$ (c) $\phi = 0.9$

Figure 4: How three players behave under different reputation influential powers of the adversary.

reduce the probability of leaking privacy. Once the application behaves nicely, the user would prefer to release its sensitive data in order to obtain better customized services. However, during this process, the behavior of the adversary cannot be controlled by the reputation influential power of the application as it depends on θ and other parameters affecting its expected utility.

Figs. 4 (a) (b) (c) illustrate how the three players behave under different reputation influential powers of the adversary, i.e. ϕ, when $\theta = 0.1, 0.5$, and 0.9, respectively. Notice that in all subfigures, the increase of θ results in the decline of q_d and q_u and the ascent of q_p. This is because a larger θ implies that the adversary pays more attention to the trust from the application, making it hide the identity of the application with a higher probability to reduce q_d. Once the chance of exposing malicious behaviors shrinks, the application is more likely to sell sensitive data for maximizing its profit. At this time, the best strategy of the user is to reduce the private data release.

One question might be raised: if increasing the reputation influential power of the application to a large extent, can we solve the privacy leakage problem easily? In fact, whether we can resolve the issue depends on the relative reputation influential power of the application rather than an absolute one. Assume that if the reputation influential power of the adversary (θ) is also large, even though the application knows the consequence would be severe once it is caught by the user due to the large ϕ, it would still leak private information because a large θ can make the adversary shield the private data safely. In other words, the mutual restriction between the reputation influential power of the application and that of the adversary is the key to determine the development of the application ecosystem.

In the following, we report the numerical analysis results for the first special case as the second special case in which the user hardly detects the malicious application cannot be solved at management level, as explained in Section 7.

Fig. 5 illustrates how the strategies of the user and the application change with the reputation influential power of the application, under different Q and $m(s_d)$. Other parameters are set to be the same as those in Figs. 3 and 4. All the subfigures demonstrate the following two common features: (1) with the increase of ϕ, q_u rises up while q_p goes down; (2) the optimal strategies of the user and the application are both binary, i.e., either 0 or 1. The reason for the first feature is obvious: the reputation influential power of the application enjoys the *"light side"* to maintain a healthy development of the application ecosystem. The second feature stems from

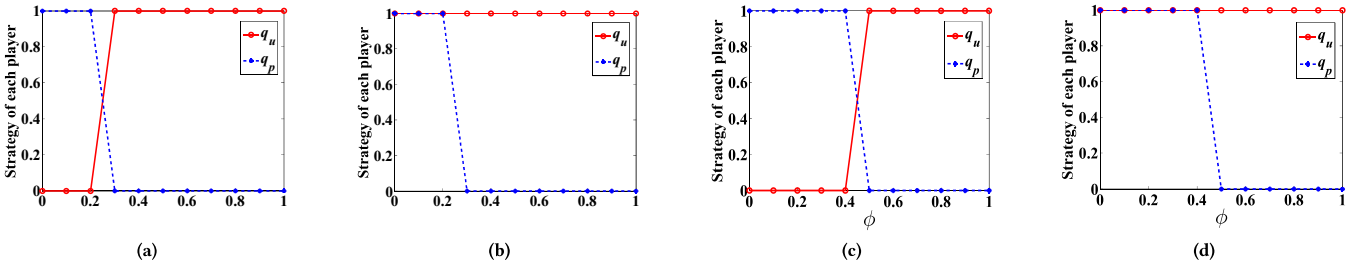


Figure 5: How the user and the application behave under different reputation influential powers of the application, where (a) $Q = 1.5$, $m(s_d) = 0.15$; (b)$Q = 15$, $m(s_d) = 0.15$; (c) $Q = 1.5$, $m(s_d) = 0.3$; (d) $Q = 15$, $m(s_d) = 0.3$.

the following fact: once the malicious application exposes itself in any condition, its strategy totally depends on whether the profit from selling private data is greater than the financially equivalent reputation loss. If the former is larger, the malicious application would sell the sensitive data without hesitation and otherwise, it would not. A similar situation happens on the user side: if the service provided by the application is attractive enough (making the profit from the service larger than the loss from privacy leakage), it would release the sensitive data; otherwise, it would not.

According to Fig. 5, one can see that lacking one player in the first special case makes no opponent fight against the *"light side"*. Hence, in this case, as long as the reputation influential power of the application is large enough, the application ecosystem can be guaranteed to be healthy.

9 CONCLUSION

Personalized applications often require users to sacrifice privacy for obtaining services. However, some ill-intentioned applications, driven by monetary profit, provide the private data to malicious third-parties without users' consent. To depict this scenario, we propose the concept of *application ecosystem*, which consists of the three entities involving privacy leakage, namely user, application, adversary. By analyzing the service trade between the user and the application, as well as the data trade between the application and the adversary, we find that there exist two inner tension forces in the application ecosystem, i.e., the reputation influential powers of the application and the adversary working as its *"light side"* and *"dark side"*, respectively. In this paper, we employ a quantum game to model the application ecosystem, taking advantage of two entanglement degrees to depict the powers of the light side and the dark side and then study their impacts on the behavior of each entity in the application ecosystem. In addition, we utilize a similar approach to analyze two special cases that may appear in typical application ecosystems. As supplements, such analyses make our study complete. Our work provides a theoretical foundation for designing effective and efficient privacy preservation solutions at the management level. To the best of our knowledge, we are the first to quantize the privacy leakage issue. Our simulation results quantitatively demonstrate how the forces of the light side and the dark one determine the strategy of each player in the application ecosystems of the general case and a special case.

ACKNOWLEDGMENTS

This work has been supported by the National Natural Science Foundation of China (No. 61472044 and No. 61472403), and the Fundamental Research Funds for the Central Universities (No.2014KJJCB32).

REFERENCES

[1] Simon C Benjamin and Patrick M Hayden. 2001. Multiplayer quantum games. *Physical Review A* 64, 3 (2001), 030301.
[2] Charles H Bennett and David P DiVincenzo. 2000. Quantum information and computation. *Nature* 404, 6775 (2000), 247–255.
[3] Xin Chen and Sencun Zhu. 2015. DroidJust: Automated functionality-aware privacy leakage analysis for Android applications. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, New York City, USA, 5.
[4] Tatjana Curcic, Mark E Filipkowski, Almadena Chtchelkanova, Philip A D'Ambrosio, Stuart A Wolf, Michael Foster, and Douglas Cochran. 2004. Quantum networks: from quantum cryptography to quantum architecture. *ACM SIGCOMM Computer Communication Review* 34, 5 (2004), 3–8.
[5] Meyer A David. 1999. Quantum strategies. *Physical Review Letters* 82, 5 (1999), 1052.
[6] Kalyanmoy Deb, Amrit Pratap, Sameer Agarwal, and TAMT Meyarivan. 2002. A fast and elitist multiobjective genetic algorithm: NSGA-II. *IEEE transactions on evolutionary computation* 6, 2 (2002), 182–197.
[7] Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. 2011. PiOS: Detecting Privacy Leaks in iOS Applications.. In *NDSS*. 177–183.
[8] William Enck, Peter Gilbert, Seungyeop Han, Vasant Tendulkar, Byung-Gon Chun, Landon P Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N Sheth. 2014. TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS)* 32, 2 (2014), 5.
[9] R. Gilmore. 1974. Baker-Campbell-Hausdorff formulas. *J. Math. Phys.* 15, 12 (1974), 2090–2092.
[10] Paul W Glimcher. 2002. Decisions, decisions, decisions: choosing a biological science of choice. *Neuron* 36, 2 (2002), 323–332.
[11] Michaela Götz, Suman Nath, and Johannes Gehrke. 2012. Maskit: privately releasing user context streams for personalized mobile applications. In *Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data*. ACM, 289–300.
[12] Michael C Grace, Wu Zhou, Xuxian Jiang, and Ahmad-Reza Sadeghi. 2012. Unsafe exposure analysis of mobile in-app advertisements. In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 101–112.
[13] Peter Hornyack, Seungyeop Han, Jaeyeon Jung, Stuart Schechter, and David Wetherall. 2011. These aren't the droids you're looking for: retrofitting android to protect data from imperious applications. In *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 639–652.
[14] Eisert Jens, Martin Wilkens, and Maciej Lewenstein. 1999. Quantum games and quantum strategies. *Physical Review Letters* 83, 15 (1999), 3077.
[15] H. Li, J. Du, and S. Massar. 2003. Continuous-variable quantum games. *Physics* 306, 2-3 (2003), 73–78.
[16] Luyun Li, Shengling Wang, Junqi Guo, Rongfang Bie, and Kai Lin. 2016. Extensive form game analysis based on context privacy preservation for smart phone applications. In *The 11th International Conference on Wireless Algorithms, Systems, and Applications*. Springer, 389–400.

[17] Ben Niu, Qinghua Li, Xiaoyan Zhu, Guohong Cao, and Hui Li. 2014. Achieving k-anonymity in privacy-aware location-based services. In *INFOCOM, 2014 Proceedings IEEE*. IEEE, 754–762.
[18] Russell Paulet, Md Golam Kaosar, Xun Yi, and Elisa Bertino. 2014. Privacy-preserving and content-protecting location based queries. *IEEE transactions on knowledge and data engineering* 26, 5 (2014), 1200–1210.
[19] Edward W Piotrowski and Jan Sladkowski. 2003. Quantum english auctions. *Physica A: Statistical Mechanics and its Applications* 318, 3 (2003), 505–515.
[20] David H. Von Seggern. 2016. *CRC Standard Curves and Surfaces with Mathematica* (3 ed.). CRC Press.
[21] Wei Wang and Qian Zhang. 2014. A stochastic game for privacy preserving context sensing on mobile phone. In *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*. IEEE, 2328–2336.
[22] Yu Wang, Dingbang Xu, Xiao He, Chao Zhang, Fan Li, and Bin Xu. 2012. L2P2: Location-aware location privacy protection for location-based service. In *The 31st Conference on Computer Communications (INFOCOM)*. 1996–2004.
[23] Zhemin Yang, Min Yang, Yuan Zhang, Guofei Gu, Peng Ning, and X Sean Wang. 2013. Appintent: Analyzing sensitive data transmission in android for privacy leakage detection. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 1043–1054.
[24] J. Zhou, Y. Li, and M. Lei. 2006. Multiplayer quantum game with continuous variable strategies. *Chinese Journal of Quantum Electronics* 23, 2 (2006), 173–177.
[25] Yajin Zhou and Xuxian Jiang. 2012. Dissecting android malware: Characterization and evolution. In *2012 IEEE Symposium on Security and Privacy*. IEEE, 95–109.

Appendix

A.1. Calculation of $J^\dagger a_u J$.

Let $A = y_1(a_u^\dagger a_p^\dagger - a_u a_p) + y_2(a_p^\dagger a_d^\dagger - a_p a_d)$. Thus, $J^\dagger a_u J = \sum_{n=0}^{\infty} \frac{1}{n!}[A^{(n)}, a_u]$. According to the properties of commutation, namely, $[A^{(0)}, B] = B$, $[A^{(n)}, B] = [A, [A^{(n-1)}, B]]$, and $[a_u^\dagger, a_u] = -1$, $[a_u, a_u^\dagger] = 1$, $[a_p^\dagger, a_u] = [a_d^\dagger, a_u] = [a_u, a_u] = [a_p, a_p] = [a_u, a_u] = [a_p, a_u] = [a_d, a_u] = 0$, the following results can be deduced:

when $n = 0$, $[A^{(0)}, a_u] = a_u$;

when $n = 1$, $[A^{(1)}, a_u] = [y_1(a_u^\dagger a_p^\dagger - a_u a_p) + y_2(a_p^\dagger a_d^\dagger - a_p a_d), a_u] = -y_1 a_p^\dagger$;

when $n = 2$, $[A^{(2)}, a_u] = [A, [A^{(1)}, a_u]] = [y_1(a_u^\dagger a_p^\dagger - a_u a_p) + y_2(a_p^\dagger a p_d^\dagger - a_p a_d), -y_1 a_p^\dagger] = y_1^2 a_u + y_1 y_2 a_d$.

when $n = 3$, $[A^{(3)}, a_u] = [A, [A^{(2)}, a_u]] = [y_1(a_u^\dagger a_p^\dagger - a_u a_p) + y_2(a_p^\dagger a_d^\dagger - a_p a_d), y_1^2 a_u + y_1 y_2 a_d] = -y_1(y_1^2 + y_2^2) a_p^\dagger$.

By a similar approach, we can deduce $[A^{(i)}, a_u]$ for any arbitrary i. As a result, the form of $J^\dagger a_u J$ can be inferred.