JAIST Repository
https://dspace.jaist.ac.jp/

Title	Analysis of membership sharing in digital subscription services
Author(s)	Xiang, Jianwen; Ogata, Kazuhiro; Futatsugi, Kokichi
Citation	Technical memorandum (School of Information Science, Japan Advanced Institute of Science and Technology), IS-TM-2007-005: 1-26
Issue Date	2007-03-16
Type	Others
Text version	publisher
URL	http://hdl.handle.net/10119/8444
Rights	
Description	テクニカルメモランダム（北陸先端科学技術大学院大学情報科学研究科）

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY

Japan Advanced Institute of Science and Technology

Analysis of Membership Sharing in Digital Subscription Services

Jianwen Xiang, Kazuhiro Ogata, Kokichi Futatsugi

Graduate School of Information Science
Japan Institute of Advanced Science & Technology
March 16, 2007
IS-TM-2007-005

Analysis of Membership Sharing in Digital Subscription Services

Working Report*, March 16, 2007

Jianwen Xiang, Kazuhiro Ogata, Kokichi Futatsugi
Graduate School of Information Science
Japan Advanced Institute of Science and Technology (JAIST)
1-1 Asahidai, Nomi, Ishikawa 923-1292, Japan
{jxiang, ogata, kokichi}@jaist.ac.jp

March 22, 2007

Contents

1 Introduction 2

2 Problem Domain Analysis of Sharing 4
2.1 Why subscription pricing . . . 4
2.2 Why sharing becomes a problem . . . 5
2.2.1 Informal description . . . 5
2.2.2 Formal analysis . . . 6
2.3 What are the difficulties to prevent sharing . . . 8

3 Incentives-Based Secretes Protection System 9
3.1 Preliminary analysis of sharing . . . 9
3.2 Basic scheme of IBSPS for friendship sharing . . . 10
3.3 Setting IBSPS for joint-purchase . . . 15
3.4 A possible revision of IBSPS . . . 17

4 User's Behavior Analysis with IBSPS 18

5 Producer's Revenue Analysis with IBSPS 21

6 Concluding Remarks 23

7 Acknowledgements 24

*This is a report, not a paper. As a report it collects thoughts, ideas, experiments, formal models, observations, etc. This report may be the basis for a publishable paper.

Abstract

A common problem to current digital subscription services is how to prevent membership (e.g., account and password) sharing beyond authorized consumers. Unlike traditional subscription services such as telephone examples, there are two main factors, namely access portability and identification transferability, which make sharing much easier and more efficient in a digital world. Moreover, there are a number of experiments and studies which disclose that both producers and consumers prefer subscription to pay-per-use to some extent with respect to digital goods, which means that we could not simply use pay-per-use as for the solution. In addition, current technical solutions and legal measures also encounter some difficulties to solve the membership sharing problem, such as how to detect the difference in the physical identity of the user. In this article, we first present a comprehensive analysis of the problem domain of sharing with respect to the aforementioned issues in terms of formal game theory and some corresponding technical, economic, and legal arguments. An incentives-based secrets protection system (IBSPS) is then proposed to encourage consumers to keep their memberships private rather than to share them among friends. Analysis of user's behavior and producer's revenue with IBSPS are also presented afterwards by introducing some corresponding utility functions.

1 Introduction

In the past several years there has been an increasing interest in developing digital rights management systems (DRMSs), which make it possible for commercial publishers to distribute digital content, such as music and movie, electronically and safely. From the point of view of the content producers, they want to utilize DRMSs to distribute and sell products in a more efficient and cost-effective way, without destroying the copyright holder's revenue stream, i.e., trying to make any kind of illegal sharing and copying impossible by both technical and legal protection measures. However, these methods usually contradict and harm the consumers' concerns to some extent, such as portability and fair use. In other words, current DRMSs do not take a good balance between the rights protection and convenient personal uses, and it can significantly reduce easy of use and may go *too* far by preventing generally accepted uses as concluded in [14].

In this article, we focused on a special issue in digital rights management (DRM), namely membership (e.g., account and password) sharing in digital subscription services. Unlike digital content files that can be typically protected from illegal copying by enforcing encryption, licenses management, and/or other methods, membership sharing is especially a problem for producers who support subscription (fixed fee) pricing for digital contents (e.g., music, movies, and journals). The problem is that it is easy and convenient to share a membership among a group of similar minded people in a digital world, and such a kind of sharing is generally difficult to be prevented or deterred by means of current technical and legal solutions.

There are two main factors which make membership sharing popular in a digital world, namely access portability and identification transferability. By *access portability* we understand that authorized users can enjoy the service through a variety of devices (e.g., laptops, desktops, MP3 player, and so on) anytime and anywhere (pro-

vided that there is such an available device). However, portability also brings about an "unexpected" effect, that is, unauthorized users can also enjoy the service through a number of different devices, which makes such a kind of sharing more convenient and efficient. By *identification transferability* we mean that the identifications (e.g., passwords and certificates) mostly used for the authentication and current membership management can be easily transferred (shared) among a group of similar minded people without the producer's knowledge[1].

Since it is difficult to detect the difference in physical identities (in which we assume that biometric authentication techniques are not widely adopted in digital content subscription services), the only way to prevent sharing is to restrict portability, which inevitably contradicts the user's satisfaction, and even more, the nature of the digital content and service per se (to some extent).

Although membership sharing seems similar to the cases that people usually share their purchased physical books or CDs among friends in a traditionally legitimate way, it does violates most of the terms of services which usually state like that "each subscriber agrees that not to allow others use her/his member name, password, and/or account." To this end, the structure of current DRM applications may drive users seeking to engage in customary personal uses of copyrighted works toward legally *questionable* behavior, and the act of sharing could involve defeating a combination of technical and contractual access control measures as pointed out by Mulligan et al. in [11].

Unfortunately, there are also some difficulties for the providers to make a *plausible* claim against such membership misuses, such as how to detect the difference in physical identities, and to meet some relatively high damage threshold [11]. For example, according to the Computer Fraud and Abuse Act (CFAA), plaintiffs pursuing a civil claim must allege damage or loss of $5000 or more in a one-year period. This is the reason that in practice, with respect to non-serious cases, the providers usually prefer contractually reserved self-help measures (e.g., revoking suspicious accounts) to law.

From an economic point of view, if sharing of subscription could not be effectively prevented, then only supporting per-use pricing seems to be a good solution for the producers. However, there is substantial evidence both from observing marketplace evolution and from surveys that consumers overwhelmingly prefer subscription pricing, likewise there are some reasons for the producers to also like subscription plans [4]. Such dilemma somehow discloses the fact, that is, so far the producers have to support subscription pricing even they do somewhat dislike sharing. We will further analyze this issue later.

Therefore, in the work described here, we first present a comprehensive analysis about membership sharing problem of digital subscription services in Section 2. The analysis is intended to answer three fundamental questions, i.e., why subscription cannot be simply replaced by per-use pricing as for solution, why sharing becomes a problem in a digital world, and what are the difficulties to prevent sharing by means of current technical and legal measures. Based on the analysis, a novel incentives-

[1] Although biometric authentication techniques such as fingerprint, face, and/or retina identification (with smart cards) are now possible and available, when and how the users and producers would like to embrace them in DRM is still in question. This is a complex issue related to cost, privacy, and industry (national or international) standards, and so far the dominant solution is still simple password (certificate) authentication. We omit this issue because it is outside the scope of this article.

based secrets protection system (IBSPS) is then proposed in Section 3 to encourage consumers to keep their memberships private rather than to share among friends. Section 5 analyzes how a producer can make profit with IBSPS. Finally, we present some further discussions and concluding remarks in Section 6.

The work presented in this article is an extension of our previous work [17], which firstly proposed the basic lottery idea to protect the secrets (memberships) from sharing. The improvements of this article are as follows. Firstly, by introducing formal game theory and utility functions of subscription services, a more comprehensive analysis of the problem domain of sharing is presented. Secondly, the basic IBSPS proposed in [17] is extended to catch both friendship sharing and joint-purchases in this article, with some revised implementation mechanisms and considerations. Last but not least, analysis of users behaviors as well as producers revenue with IBSPS are also presented in this article so as to make the solution more practical and complete.

2 Problem Domain Analysis of Sharing

In this section, we focus on the problem domain analysis of membership sharing in digital subscription services. More specifically, our main interests are the following three key questions:

- why *subscription pricing* is important (necessary) for digital goods,
- why sharing only becomes a problem in a *digital* world, and
- What are the *difficulties* to prevent sharing in terms of current technical solutions and legal measures?

The answers to these three questions consist of the motivation and significance of this article.

2.1 Why subscription pricing

In this section we present a brief analysis of subscription and per-use pricing, and analyze why both consumers and producers prefer the former to the latter to some extent with respect to digital (information) goods. This discloses the fact that to avoid sharing and potential revenue loss, the producers cannot simply just support per-use pricing as for the solution.

First, there is considerable evidence of consumer preferences for subscription over per-use pricing in traditional business areas. Many of the examples come from telephone and cellphone service experiments. For instance, during the 1970s, the Bell System started offering customers a choice between the traditional flat rate option and a measured rate option. The former costs $7.50 per month and allows unlimited local calling, while the latter costs a basic charge of $5.00 per month which allows first 50 free local calls, and then costs $0.05 per call. It is obviously that anyone making fewer than 100 local calls per month would be better off with the latter, i.e., the measured rate option. However, numerous experiments show that over 50% of the consumers

who chose the flat rate plan actually made less than 50 local calls, which is covered by the measured rate basic charge [2, 5, 6]. Similar cases can also be found in the choices made by consumers signing up for various plans that providing more calling than they actually used [10]. In the online service area, it has also been common that consumers usually pay for larger blocks or much more time than they actually used, and that is the reason that most consumers prefer subscription pricing for Internet access and/or entertainment site subscription services.

According to [2, 5, 6], there are three main reasons that probably lead consumers to prefer flat-rate pricing: (1) Insurance: flat-rate pricing provides protection against sudden large bills; (2): Overestimate of usage: consumers typically overestimate how much they use a service, with the ratio of their estimate to actual usage following a long-normal distribution; (3) Hassle factor: In a per-use situation, consumers keep worrying whether each call is worth the money it costs, and it has been observed that their usage goes down. A flat-rate plan can relieve them from such worries. All these three factors could be regarded as part of a general preference by consumers for simple and predictable pricing [4].

In addition to getting extra profit from consumers overestimation of their usages, there are other two main reasons for producers to also like subscription pricing, i.e., locking and developing close relations with consumers [4]. Although generally speaking, unlike software where network externalities are important, digital entertainment and information goods, such as music, movies, and journals, usually need not to concern the factor of network externalities very much, it is still the producer's interests to lock and develop close relations with the consumers by subscription pricing and/or site licensing. In addition, producers of such entertainment and informal goods typically have an imperfect monopoly on their products [4], which means that consumers are easy to find and switch to other substitutes, e.g., similar goods provided by their opponents. From this point of view, subscription is also better than per-use pricing since the latter does repress usage [6] and is difficult to cultivate regular and loyal customers.

2.2 Why sharing becomes a problem

2.2.1 Informal description

As analyzed in Section 2.1, even if we ignore the factor that there is substantial evidence from both observing marketplace evolution and surveys that most customers prefer subscription pricing, per-use pricing is likely to be dominated by subscription pricing when the consumer and producer preference effect is taken into account. However, the survey result of the online music industry in 2003 [3] is somehow inconsistent with the above analysis. In this survey report, it seems that pay-per-use pricing rather than subscription was dominant for both downloading and streaming media (music)[2].

To our understanding, the worry about membership sharing is one of the main factors resulting in the difference (inconsistency). If this conjecture holds, then it brings about another question, that is, why sharing becomes a (big) problem in a digital world. Similarly, we could ask a relative question, that is, why sharing seems to be a trivial

[2]It should be noted that the total number of respondents ($N = 6$) in [3] is rather low despite the relatively high return rate (30%), and thus the result allows only a descriptive presentation.

issue with respect to traditional subscription services and products, such as telephone, public/private club, library, and so on.

There are two factors that make digital subscriptions different from traditional ones, namely *access portability* and *identification transferability* as discussed in Section 1. For instance, with respect to the telephone example, a consumer enjoyed by a flat-rate plan can occasionally lend (not share) her (stationary) telephone to her neighbors or friends for casual uses, but it is difficult or intolerable for her to share the telephone with her neighbors and/or friends whenever they want to use the telephone. Here, the hindrance to sharing is that the access tool, i.e., the telephone itself is not portable. Taking another public/private club and library example, in which each subscribed member is typically authenticated by a corresponding membership card with a recent photo of the owner, this makes it difficult to share (transfer) the identification (card) to others.

However, with respect to the digital subscription services, the situation changed, i.e., people can share their memberships more *conveniently* and *efficiently* in a digital world than in a traditional "physical" world due to the same two factors, i.e., access portability and identification transferability. On one hand, network and portable devices make not only accessing but also sharing much more conveniently and efficiently. As described in [16], the relationship between copyright and what consumers expect is a "fundament trade-off between control and customer value," and thus the portability — a normative use of customer expectation —- cannot be unilaterally prevented by the producers by force. On the other hand, current dominant password (certificate) authentication makes it difficult to detect the differences in the physical identities, and thus it makes it possible to transfer (share) such text-based identifications among a group of similar-minded people without the knowledge of the producers.

2.2.2 Formal analysis

To analyze the behaviours of sharing and not sharing in a formal way, we refer to formal C/P games [15] and use the terms of conversion and preference for sharing as follows.

We suppose that:

- $\mathcal{A}$ is a non-empty set of agents (consumers).
- $\mathcal{S}$ is a non-empty set of strategies (called as synopses in [15]) consisting of the following two strategies in general:
  - s_n denotes the strategy of not sharing;
  - s_s denotes the strategy of sharing;
- For $a \in \mathcal{A}$, $\succ_a$ is a binary relation over $\mathcal{S}$, associating two (different) strategies if agent a can convert the first to the second. For example, $s_n \succ_a s_s$ represents that consumer a can *convert* not sharing to sharing;
- For $a \in \mathcal{A}$, $\lhd_a$ is a binary relation over $\mathcal{S}$, associating two (different) strategies if agent a prefers the second to the first. For example, $s_n \lhd_a s_s$ represents that consumer a *prefers* sharing to not sharing.

And we also assume that:

- U_n is the utility from not sharing.
- U_s is the utility from sharing.
- P is a predicate denoting that the access of the service is portable;
- T is a predicate denoting that the identification used for authentication of the service is transferable.

We can therefore derive the following two equations:

$$P \wedge T \Rightarrow s_n \succ_a s_s \tag{1}$$

i.e., a consumer, a, can convert to sharing (not occasionally lending) if the the access of the service is portable and the identification used for authentication is transferable (we suppose that $\Rightarrow$ is the logic implication operator).

$$U_s > U_n \Rightarrow s_n \lhd_a s_s \tag{2}$$

i.e., a consumer, a, prefers sharing to not sharing if the utility of sharing is bigger than not sharing.

Moreover, we define a (free) change-of-mind relation $\rightarrow_a$ such that $\rightarrow_a \triangleq \succ_a \cap \lhd_a$, and therefore we can derive an equation for the change-of-mind for sharing as follows:

$$(P \wedge T) \wedge (U_s > U_n) \Rightarrow s_n \rightarrow_a s_s \tag{3}$$

i.e., a consumer will actually bring sharing into effect if sharing is both convertible and preferable.

As seen from Eq.(1 - 3), with respect to traditional subscription services, since the condition for the conversion to sharing (i.e., $P \wedge T$ in Eq.(1)) is typically difficult (or impossible?) to meet, the producers do not need to worry much about the problem of sharing (i.e., Eq.(3) holds) even though some consumers may prefer sharing (i.e, Eq.(2) holds). However, the situations changed in a digital world, and the reality of digital subscription services makes it difficult (or impossible) to negate the condition of the conversion equation (i.e., $\neg P \vee \neg T$) as discussed in Section 1 and Section 2.2.1. Therefore, to prevent (or effectively deter) sharing, the only solution is to make the utility from not sharing bigger than from sharing (i.e., $U_n > U_s$). Since the utility can be typically further defined as a function relating to a variety of factors, such as the price p, friendship f, willingness to pay θ, and the satisfaction of usage time s_t, this can be done by introducing new factors such as (additional) incentives into the utility function. We will further discuss this issue in Section 3.

2.3 What are the difficulties to prevent sharing

Continue the discussion of the last subsection, we further illustrate a number of current technical and legal solutions to solve the sharing problem, and discuss some potential troubles of these solutions.

Examples of possible technical solutions and attempts to the membership sharing problem are:

- prohibiting simultaneous access with the same account,
- binding each account with specific limited numbers of devices,
- monitoring suspicious sharing with "abnormal" frequent logins (e.g., an account has been logged in from more than 5 different computers within 48 hours),
- deterring sharing with the analysis of keystroke biometric data [8], and so on.

These example techniques, all seem to focus on preventing the conversion condition of sharing. The first three try to deter the access portability to some extent, and the last attempts to prohibit identification transferability so as to solve the sharing problem.

A fundamental *tradeoff* between control and user's satisfaction should be made with respect to the above conversion-oriented solutions. In other words, the limitation to convertability will inevitably harm the user's satisfaction to some extend. And generally speaking, we cannot prevent the conversion completely since it is somehow a "nature" of the network.

Consequently, a potential trouble of the conversion-oriented techniques is that how to determine an *appropriate* threshold to distinguish normal and abnormal uses. For example, how many devices should be granted for one membership such that most of the users would be satisfied in terms of their normal uses? This is not a simple question, and the answer (tradeoff) always implicitly implies that sharing is somewhat possible (allowed). And even in an extreme case, e.g., only one specific device is granted to access the service, several similar minded people can still share the membership with the common device to some extent due to the identification transferability.

Another fact is that current text-based passwords (certificates) can be easily shared among a number of users without the producer's privity and consent, which makes it very difficult to detect the difference in physical identities behind the devices. This is also a difficulty in terms of current legal measures which we will discuss later.

In addition, it seems that there are some technical problems to prevent simultaneous access with respect to some distributed environments such as P2P networks. This problem has been reported by MusicAlly in 2005, which said that sharing of Napster passwords was popular among youngsters because that simultaneous access was not really prohibited as claimed by the content provider [12].

Generally speaking, there are two main difficulties to solve the sharing problem in terms of current legal measures. The first is that, as mentioned before, how to detect the difference in physical identities behind the devices. The other is to meet some relatively high damage threshold as discussed in the Introduction section. These two factors make it difficult for producers to make a plausible claim against sharing. Therefore, with regard to non-serious cases, producers usually prefer contractually reserved

self-help measures to law. The legal issues about sharing are quite subtle, and for a detailed analysis and discussion, we refer to [11].

Unlike the conversion-oriented techniques mentioned above, our main interest is to propose a preference-oriented method to solve the sharing problem, i.e., how to increase consumer's preference for not sharing rather than sharing in terms of some positive incentives for the consumers. We do not think that the comparison of these two kinds of techniques is important, since they are somehow orthogonal in terms of different considerations. Instead, we think that the combination of them could be a more effective solution since both of them have their own merits and constraints with the common goal.

It should also be noted that we do not want to use IBSPS to replace current terms-of-use policies, or other legal, technical protection measures. Rather, we aim to add IBSPS as an additional layer of protection for digital rights management (DRM) systems that already have such safeguards.

3 Incentives-Based Secretes Protection System

3.1 Preliminary analysis of sharing

We start by considering how a user can obtain the subscription service by different ways. Suppose that there is a continuum of potential users who are characterized by their willingness to pay (valuation), θ, for the subscription service. We assume that θ is uniformly distributed on the interval $[0, 1]$. Suppose that the price of the service is p, a user can generally obtain the subscription service in three different ways:

- One is to buy the legitimate service at price p when $\theta \geq p$, and we call such a user as a *buyer*;
- The other is to use a shared membership freely from his/her friends, and we call such a user as a *(free) sharer*;
- Another possibility is to buy the service through a kind of joint-purchase, in which we call such a user in the joint-purchase as a *co-buyer*.

A sharer can get a free membership from either a "kind" buyer, or a co-buyer, or even a sharer who knows the membership from another buyer, co-buyer, or sharer. The first case, i.e., sharing between a sharer and an original buyer, could be regarded as a kind of "first-hand" sharing, and we call it as *friendship sharing*. Similarly, joint-purchase could also be regarded as a kind of first-hand sharing, since it occurs among several original co-buyers. In contrast, the further sharing occurring between a sharer and some co-buyer/sharer could be regarded as a kind of "second-hand" sharing, since the sharing provider, i.e., the co-buyer/sharer, has already taken part in one sharing before providing the membership to the sharing consumer, i.e., the sharer. In this article, we devote our attention to the two kinds of first-hand sharing, i.e., friendship sharing and joint-purchase, since the second-hand sharing can only occur when the first-hand one occurs.

A buyer can choose to provider sharing or not depending on his/her own interest. To this end, we further divide all the buyers into two sub-classes, i.e., "*dishonest*" and "*honest*" buyers. The former are the buyers who "kindly" share their memberships with friends, while the latter are those who behave honestly according to the terms of services, i.e, not sharing.

Unlike friendship sharing that always damages the producer's revenue, joint-purchase has actually two folds. On one hand, the joint-purchases among potential consumers with higher evaluations for the service ($\theta \geq p$) do somewhat decrease the revenue stream of the service provider; But on the other hand, the joint-purchases among users with lower evaluations ($\theta < q$) can somewhat increase the revenue stream, otherwise these users will simply not buy the service since their respective willingness to pay is less than the price. And in this case, we typically assume that their total evaluation is greater than the price.

In addition to its dualism, joint-purchase is generally more difficult to be handled with in terms of some incentives-based methods. This is because the co-buyers participating some joint-purchase can also make a deal to share the incentives, just as how they share the price and usage time of the service. This situation does not happen with respect to friendship sharing, since the buyer would like to keep the membership private as long as the provided incentives are somehow attractive enough than the friendship earned from sharing.

The formal analysis of user's behavior will be discussed later in Section 4, such that it is more clear to compare the difference of user's behavior between without and with our proposed method. And in the following sections, we will first present an incentives-based secrets protection system (IBSPS) to solve the sharing problem, and then further analyze the user's behavior as well as the provider's revenue stream with our proposed IBSPS.

3.2 Basic scheme of IBSPS for friendship sharing

For clarity, we first consider the case of friendship sharing, and then discuss the case of joint-purchase in the next section. We limit the basic scheme of IBSPS to the following situations: The provider offers online subscription services of streaming media, and supports fixed period pricing methods such as monthly and yearly subscriptions (pay-per-use is not considered because generally the one-off identification or access needs not to be protected); Concurrent access of one membership is technically prohibited, while there is not necessary to restrict the access portability, i.e., a consumer can enjoy the streaming media and service with the identification on any computers (devices) that he/she possesses or likes.

Informally speaking, IBSPS can be understood as a kind of lottery to stimulate the consumers to keep their secrets private, and it can be briefly divided into the following three phases:

1. During the *Subscription* phase, the consumer (buyer or co-buyer) subscribes the service and receives a secret (e.g., an account and password pair) that allows access to the protected service and content. The provider also registers the password to an escrow service and places an amount of money as the prize of lottery

into an escrow account.

2. During the *Registration* phase anyone who has a copy of the password can register to the escrow service, by providing proof of knowledge of the password.

3. During the *Lottery* phase anyone who provided proof in the registration phase are given a chance to win the prize in the escrow.

And to state the model more formally, we define the parties and variables used in IBSPS as shown in Table 1. The formal details of IBSPS are as follows.

Variable	*Description*
P	The service provider
E	A trusted escrow service
$B_1 \dots B_m$	Buyers
$S_1 \dots S_n$	Sharers
Z	The total prize set for lottery
ϕ_{B_i}	The identification to B_i $(i = 1, \dots, m)$
$d(\phi_{B_i})$	The textual description of ϕ_{B_i}
$H(\phi_{B_i})$	The hash of ϕ_{B_i}
τ	End time of identification protection
p	The price of the service (secret)

Table 1: Variables used in IBSPS

Phase 1: Subscription. Firstly, the buyers $B_1 \dots B_m$ subscribe the service by paying the price of the service p to the provider P, and then receive the secrets (identifications) $\phi_{B_i} (i = 1, \dots, m)$ from P, respectively. These two steps (i.e., paying and receiving) can be done in a fare exchange manner such as described in [1, 18], but here we do not require a specific mechanism since it is not the main focus of IBSPS.

After that, P sends a list of hash values and descriptions of the secrets as well as the ending time to E, denoted by $d(\phi_{B_i})$, $H(\phi_{B_i})$ $(i = 1, \dots, m)$, and τ, respectively [3]. The hash value will serve as a proof of possession of ϕ_{C_i} without revealing the secret to the escrow service.

Finally, the provider P places an amount of money, say Z, as the prize of lottery into a trusted escrow service E. The amount of the money of the prize Z, can be generally defined as a function of the total number of buyers (m) and the price of the service (p) such as in a form of $Z = \lambda \cdot mv$, in which we suppose that λ is an coefficient ranging between $(0, 1)$.

Therefore, phase 1 can be concluded as follows:

$$
\begin{array}{lrcl}
(1) & B_i \rightarrow P & : & v \quad (i = 1, \dots, m) \\
(2) & P \rightarrow B_i & : & \phi_{B_i} \\
(3) & P \rightarrow E & : & d(\phi_{B_i}), H(\phi_{B_i}), \tau \\
(4) & P \rightarrow E & : & Z
\end{array}
$$

[3] For clarity, we suppose that this group of ϕ_{C_i} have the same protection time τ, e.g., a group of consumers who subscribe the service within the same period of time (e.g., one day or one week).

Phase 2: Registration At this stage, E broadcasts widely that it is seeking *anonymous* registrations from *anyone* holding identifications described by $d(\phi_{B_i})$. Such message can also be posted on the homepages of P and E, or as a complementary clause of the terms of service of P, so as to let it be known as widely as possible.

There are two key points here. One is that the sharers $S_1 \ldots S_n$ who obtain the identifications from B_i $(i = 1, \ldots, m)$ rather than P, can also participate in this lottery. The other is the *anonymity* of the registration, which can stimulates the sharers to register without revealing their real identities and thus losing their friendships with the "kind" buyers (sharing providers). This can be implemented by using anonymous email address or other mechanisms, such that the escrow E can conform the registrations and contact with the registrants (if they win the lottery) without knowing their real identities.

The registration can be done by sending the hash value and description of ϕ_{B_i} $(i = 1, \ldots, m)$ to E, i.e., $H(\phi_{B_i})$ and $d(\phi_{B_i})$. For clarity, we suppose that $\phi_{B_{r_1}}, \ldots, \phi_{B_{r_n}}$ are variables representing any possible ϕ_{B_i} $(i = 1, \ldots, m)$, and $B_1, \ldots, B_m$ and $S_1, \ldots S_n$ all have registered. The process can be described as follows:

$$
\begin{array}{lrcl}
(5) & B_1 \rightarrow E & : & d(\phi_{B_1}), H(\phi_{B_1}) \\
 & \vdots & & \\
 & B_m \rightarrow E & : & d(\phi_{B_m}), H(\phi_{B_m}) \\
(6) & S_1 \rightarrow E & : & d(\phi_{B_{r_1}}), H(\phi_{B_{r_1}}) \\
 & \vdots & & \\
 & S_n \rightarrow E & : & d(\phi_{B_{r_n}}), H(\phi_{B_{r_n}})
\end{array}
$$

Phase 3: Lottery. The last step, beginning at the end time of τ, is the lottery process. Each registrant will have a chance to win the prize Z set by P.

To achieve a fair lottery in which sharing will be punished once it happened, the system should guarantee the following three properties:

1. If no identification (secret) has been shared and each buyer only registered once, i.e., no multiple registrations with the same hash values have been found, then each registrant can get an average possibility $1/m$ to win the prize.

2. In case an identification has been registered more than once, then all the registrations with the same hash value should be degraded, i.e., each registrant of the multiple-registration must receive a (much) lower possibility than $1/m$.

3. In addition, the total sum of the possibilities of the registrants of the multiple-registration should still less than or equal to $1/m$, otherwise collusion would be profitable.

Recall that in Phase 2, E receives anonymous registrations with only $d(\phi_{B_i})$ and $H(\phi_{B_i})$ $(i = 1, \ldots, m)$ (as well as the anonymous contact information such as email addresses), and thus it is difficult for E to distinguish who are buyers or sharers. However, it is trivially *easy* for E to detect multiple registrations with the same hash values and descriptions.

Suppose that E classifies all the registrations by means of different hash values, and we use the term of *registration length* to denote the number of registrations with the same hash value, i.e., how many times the same hash value has been registered to the lottery. A length observer function is then defined to observe the registration length of a hash value in a form of $len(H(\phi_{B_i}))$. If $len(H(\phi_{B_i})) = 1$, then we call the corresponding registration is an *honest* registration (with length 1). If $len(H(\phi_{B_j})) = l \geq 2$, then we call all the registrations with the $H(\phi_{B_j})$ as *dishonest* registrations with length l.

For any registration, say xR (xR can be either an honest registration or a dishonest one), with a hash value $H(\phi_{B_i})$ and a length l (i.e., $l = len(H(\phi_{B_i}))$), its possibility to win the prize can be defined as follows:

$$P(xR, H(\phi_{B_i}), l) = f(l) \cdot 1/m \tag{4}$$

where we suppose that $f(l)$ is a decreasing function ranging between $[0, 1]$, and when $l = 1$, $f(l) = 1$.

The above possibility function specifies that if the buyer B_i does not share the identification with friends and B_i registers honestly (i.e., only once), then B_i can get an average possibility $1/m$ as promised by the producer. But if sharing happens, then B_i will receive a smaller possibility than $1/m$ as the punishment for providing sharing. And at the same time, the sharers can also get the same chances as of B_i to win the prize, which is a kind of extra and zero-risk wealth for them due to the anonymity of the registration. In addition, to prevent collusion and multiple registrations done by the same registrant, the following constraint of $f(l)$ must hold:

$$f(l) < \frac{l-1}{l} \cdot f(l-1) \qquad (l \geq 2) \tag{5}$$

Moreover, if we want to prevent unlimited re-registration competition between the dishonest registrants with the same $H(\phi_{B_i})$, we have to introduce a stronger constraint. The re-registration competition may happen if a dishonest registrant can make profit through one more re-registration, provided that there are other dishonest registrants share the same hash value. The stronger constraint of $f(l)$ can be defined as follows:

$$f(l) < \frac{1}{2} \cdot f(l-1) \qquad (l \geq 2) \tag{6}$$

Suppose that E finally receives u honest registrations and v sets of dishonest registrations (i.e., there are v hash values have been registered for multiple times), where $u + v = m$. We assume that the registration lengths of the hash values are $a_0, a_1, \cdots, a_v$, where $a_0 = 1$ denoting the length for all the u honest registrations, and $a_1, \cdots, a_v \geq 2$ denoting the lengths for the v sets of dishonest registrations, respectively. We also assume that an appropriate function of $f(l)$ ($l = a_0, a_1, \ldots, a_v$) has been defined beforehand, and $f(l)$ satisfies the stronger constraint (6). Let $hR_1, \ldots, hR_u$ be the u honest registrations with length 1, and $dR_1^{a_i}, dR_2^{a_i}, \ldots, dR_{a_i}^{a_i}$ ($i = 1, \ldots, v$) be the a_i dishonest registrations with the same identification of length a_i, the Phase 3 can then be concluded as follows:

$$
\begin{array}{lllll}
(7) & E & \dashrightarrow & hR_1, hR_2, \ldots, hR_u & : \ \frac{1}{m} \cdot Z \\
 & E & \dashrightarrow & dR_1^{a_1}, dR_2^{a_1}, \ldots, dR_{a_1}^{a_1} & : \ f(a_1) \cdot \frac{1}{m} \cdot Z \\
 & & & & \vdots \\
 & E & \dashrightarrow & dR_1^{a_v}, dR_2^{a_v}, \ldots, dR_{a_v}^{a_v} & : \ f(a_v) \cdot \frac{1}{m} \cdot Z
\end{array}
$$

As shown in step (7) above, an implementation issue is how to guarantee that different registrations will receive exactly the possibility of $f(l) \cdot \frac{1}{m}$ as stipulated by $f(l)$ $(l = 1, a_1, a_2, \ldots, a_v)$.

One possible implementation solution, namely a novel two-step duplication mechanism, can be used to solve the above problem. The idea is to duplicate each registration with a number of copies, and the number of copies is typically determined by the length of the hash value in an inverse ratio. In other words, more copies will be made for the registrations with smaller lengths.

1. Firstly, since the total possibility may not equal to 1 after applying $f(l)$ to each registration, we have to collect the loss of the possibility and make an "null" registration to take over it. Let the possibility of the null registration be $f(a_{nil}) \cdot \frac{1}{m}$, and the value of $f(a_{nil})$ can be calculated as follows:

$$
f(a_{nil}) = v - \sum_{k=1}^{v} f(a_k) \cdot a_k \tag{7}
$$

2. Secondly, we define a duplication function, namely $g(l)$, to specify how many copies should be made for the registrations with length l. The function $g(l)$ must satisfy that

$$
\frac{g(a_i) + 1}{g(a_j) + 1} = \frac{f(a_j)}{f(a_i)} \quad (i, j = 0, 1, \ldots, v, nil) \tag{8}
$$

   For instance, $g(a_i)$ $(i = 0, 1, \cdots, v, nil)$ can be defined as:

$$
\frac{f(a_i)}{\gcd(f(a_0), f(a_1), \cdots, f(a_v), f(a_{nil}))} - 1 \tag{9}
$$

   where gcd denotes the function of greatest common divisor.

In case the null registration and its copies finally win the prize, then the prize can be either returned back to the producer, or delivered to some charities, or kept and accumulated for the next round lottery according to different situations and agreements. An alternative to deal with the lost possibility (i.e., the punishment of sharing) is to transfer it to the honest registrants as a kind of additional award for not sharing. And in this case, each honest registrant can receive an average possibility of $(\frac{f(a_{nil})}{u} + 1) \cdot \frac{1}{m} \geq \frac{1}{m}$ to win the prize for the honest behaviour, i.e., not sharing and no multiple registrations.

3.3 Setting IBSPS for joint-purchase

In Section 3.2, we have analyzed how IBSPS can encourage buyers to keep their secrets (identifications) private rather than to share among friends. The key is that once a buyer shares, then the buyer would lost some possibility to win the prize, in which the loss is out of his/her control and knowledge. In this section, we discuss the other kind of sharing, i.e., joint-purchase, and analyze how IBSPS can also be applied to deter the joint-purchases to some extent by setting appropriate upper bound constraints for the registration length, $f(l)$.

Suppose that 2 co-buyers make an agreement to buy the subscription service: each of them pays half the price, $\frac{1}{2}p$, and shares the prize if their (joint) registration wins, i.e., the expectation value of the prize for each other is $\frac{1}{2} \cdot (\frac{1}{m} \cdot Z)$. The above agreement seems reasonable and fair, if nobody would like to register again secretly so as to get more expectation value of the prize, which is exactly the potential hole of the balance.

Recall that in the last section, we have defined the upper bound constraint for $f(l)$ (see (6)), which guarantees that if an identification has been shared among several different users, then no user would like to register more than one time since it is not profitable. In this section, we further define the lower bound constraints of $f(l)$. The intention is to encourage the co-buyers sharing one specific membership to re-register secretly for their own interests, such that the final total expectation value of the co-buyers somewhat decreases and is less than $\frac{1}{m} \cdot Z$, i.e., the average expectation value of the honest buyers.

Considering the joint-purchase with 2 co-buyers, the lower bound constraints of $f(l)$ $(l \geq 2)$ can be defined as the following two equations, depending on l is even or odd, respectively.

$$f(l) > \begin{cases} \frac{l-1}{l+1} \cdot f(l-1), & l = 2, 4, 6, \ldots, \quad (10) \\ \frac{l-2}{l} \cdot f(l-1), & l = 3, 5, 7, \ldots. \quad (10') \end{cases}$$

Constrained by the upper bound constraint (6), (10) and (10′) can only hold when $l = 2$ and $l = 3$, respectively. The value and range of $f(l)$ can thus be redefined as follows:

$$f(l) \begin{cases} = 1, & l = 1, \quad (11a) \\ < \frac{1}{2} \cdot f(l-1) \text{ and } > \frac{1}{3} \cdot f(l-1) & l = 2 \text{ or } 3, \quad (11b) \\ < \frac{1}{2} \cdot f(l-1) & l \geq 4. \quad (11c) \end{cases}$$

The above formulas say that after the first joint-registration ($l = 1$), either of the 2 co-buyers, say C_1, can still make profit through the second secret registration. And based on the assumption that C_1 has done the second registration, the other co-buyer, say C_2, has no choice but to re-register for the third time so as to grab back some expectation value of the prize. However, the total expectation value of and the possibility to win the prize of the 2 co-buyers will decrease by such selfish and "rational"

re-registrations. The analysis can be also applied to the joint-purchases with more than 2 co-buyers.

For better understanding, we present a simple example. Suppose that $f(1) = 1$, $f(2) = 2/5$, and $f(3) = 1/7$. We assume that the first joint-registration has already been done, and then there are two strategies for the co-buyers, namely not register and register again (short in N and R). The analysis can be represented in a strategic game form as shown in Table 2: (For clarity, we keep only the coefficients and omit $\frac{1}{m} \cdot Z$ of the payoffs in Table 2.)

		Co-buyer II	
		N	R
Co-buyer I	N	$1/2, \frac{1}{2}$	$1/5, \frac{3}{5}$
	R	$3/5, \frac{1}{5}$	$3/14, \frac{3}{14}$

Table 2: PD game for joint-purchase

As shown in Table 2, for both of the co-buyers, we assume that the conversion relation between not register and register again naturally holds, and vice versa, i.e., $s_N \succ s_R$ and $s_R \succ s_N$. The change-of-mind relation is then only dependent on the preference relation, i.e., more expectation value is typically preferred than the less ones. There is only one unique (change-of-mind) equilibrium, the lower-right cell, i.e., both of the co-buyers would like to change their minds and register again secretly for their own interests. It is a kind of prisoner's dilemma (PD) game, in which re-registration is the strictly dominant strategy for both of the co-buyers, regardless of that they could earn more through a collusive agreement at the upper-left cell, i.e., both of them do not re-register but share the first joint-registration. Two important and interesting properties of the game of joint-purchase are the *anonymity* of the registrations (except for the first joint registration) and the *uncertainty* of the lottery, which make it impossible or rather difficult for any co-buyer to observe the other co-buyer's strategy even after the lottery. This makes the cooperation (i.e., the collusive agreement of the first joint-registration) is much more easily to go for naught, such as what game theorists call as 'cheap talk', even in a repeated game form.

To avoid the prisoner's dilemma and unnecessary suspicion for each other's secret re-registration, the co-buyers may agree to finish the second (joint) registration jointly, such that no one would like to re-register again secretly. In this case, constrained by the upper bound constraint (6), there is no possible value of $f(l)$ can further break the agreement and balance. However, if this happens, then the co-buyers actually agree to degrade their total expectation value of the prize to some extent compared with the honest buyers. Therefore, in an average sense, we can expect that the cost-benefit (cost-prize) ratio of the co-buyers will less than those of the honest buyers. In other words, the co-buyers would mostly pay more money than the honest buyers in IBSPS. This can be served as a kind of negative factor for those who want to buy the service jointly, especially for the potential consumers whose willingness to pay are higher than the price of the service.

3.4 A possible revision of IBSPS

In the basic scheme of IBSPS (see Section 3.2), we assume that a buyer will only lose some of the possibilities to win the prize when sharing happens. And a similar assumption is also made as for the co-buyers (see Section 3.3). This may cause a problem, that is, the buyer (or co-buyer) may somehow think of that the loss is not so significant since he/she can still gets some chance to win the prize, even if the sharers (or the other co-buyers) re-register to the lottery secretly, and thus the effectiveness of IBSPS is somewhat weakened. To solve this problem, we further propose a revision of IBSPS, which removes such aleatory minds and sets the punishment for the original registrants much more seriously, i.e., they will lose all the possibilities once the others re-register to the lottery.

To achieve the above goal, the revised IBSPS can be briefly concluded by the following three revised registration principles:

- *First (registration) default*: in the step (3) of phase 1 (see Section 3.2), we assume that when the producer first sends the registration information (i.e., $d(\phi_{B_i})$, $H(\phi_{B_i})$, and τ) to the escrow, the first registration is done as for the original buyers and co-buyers by default. This can be done by requiring the producer to provide additional corresponding anonymous contacting information (e.g., email address) of the consumers to the escrow service, which can be collected in the step (1) of phase 1.

- *Second (registration) replace*: at the registration stage, i.e., phase 2, the escrow still broadcasts widely that it is seeking anonymous registrations from anyone holding the identifications. However, all the registrants are informed with that once the second registration with the same identification occurs, then the first registration will be replaced by the second one. In other words, the original registrants (i.e., buyers or representative co-buyers) will lose all the chances to win the prize.

- *Third (registration) discard*: in case more than two registrations with the same identification exist, then all the registrations with that identification will be discarded. This principle is used to prevent the original buyers and co-buyers to further register to escrow after the second registration.

In short, the intention of these three principles is to restrict the registration length less than or equal to 2, and the first (original) registration will always be replaced with the second registration. In this case, we require that $f(2) > \frac{1}{2}$ as for the joint-purchase.

For instance, suppose that the first registration is done, and thus anyone holding the identification (either a buyer, a sharer, or a co-buyer) has two strategies, i.e., not register or register again (short in N and R). For clarity, let $a = \frac{1}{m} \cdot Z$, and $\frac{1}{2}a < b < a$), the revised IBSPS for friendship sharing and joint-purchases can be represented as shown in Table 3 and Table 4, respectively:

As for the friendship sharing, the weakly dominant strategy of the buyer is not to register again, while the sharer would like to try to register since it is his weakly dominant strategy (see Table3). And once the sharer registers, the buyer would lose his benefit regardless of what kind of strategy (i.e., register or not register again) he takes.

		Sharer	
		N	R
Buyer	N	$a, 0$	$0, b$
	R	$b, 0$	$0, 0$

Table 3: Revised IBSPS for friendship sharing

		Co-buyer II	
		N	R
Co-buyer I	N	$\frac{1}{2}a, \frac{1}{2}a$	$0, b$
	R	$b, 0$	$0, 0$

Table 4: Revised IBSPS for joint-purchase

With regard to the joint-purchase, both of the co-buyers' weakly dominant strategy is to register again secretly, which makes the upper-left cell (i.e., the first joint-registration) never constitute an equilibrium in the game (see Table 4). The worst case is that both of the co-buyers register again, and then both of them will lose all the benefits.

If we consider the joint-purchase as the secondary risk of sharing due to its dualism as mentioned before, and suppose that the goal is only to deter the friendship sharing, then we could set $f(2)$ as small as possible instead of requiring that it is bigger than $\frac{1}{2}$. In this case, the sharers still have the incentives to participate in the lottery as long as $f(2)$ is not equal to 0, but the users engaged in friendship sharing (i.e., dishonest buyers and sharers) will totally receive a much less possibility to win the prize compared with the honest users in an average sense.

A potential "moral criticism" of the revised IBSPS is that it explicitly states that it is seeking dishonest registrations since the first honest registration is already done by default. Although the legitimate but dishonest buyers may thus somehow dislike such policy, the service provider can state it clearly and explicitly in the contract (terms of services) beforehand so as to avoid some potential unnecessary troubles.

4 User's Behavior Analysis with IBSPS

In this section, we further present a formal analysis of user's behavior in terms of some utility functions. The main intention is to compare the difference between the behaviors without and with IBSPS, i.e., how sharing occurs and how sharing can be somewhat prevented with our proposed method.

To analyze the user's behavior in a formal way, we use the framework proposed by Mussa and Rosen for modelling vertical (quality) differentiation [13], by considering the quality of goods as the satisfaction of usage time of the subscription service in

our model. It should be noted that the utility function presented below is just one possible model based on our own considerations, and there may exist some other more realistic models to observe the user's behavior in terms of some different observations and parameters.

For clarity, we limit our analysis to 2-person sharing/joint-purchase. In our model, we define the satisfaction of usage time of different users (i.e., honest and dishonest buyers, sharers, and co-buyers) as the quality of service gained by such users. Let $q_h = 1$ denote the quality of service gained by the honest buyers, q_d (with $0 < q_d \leq q_h$ in general) denote the quality of service of the dishonest buyers, q_s (with $0 < q_s < q_d$ in general) denote the quality of service of the sharers, and q_c (with $0 < q_c < q_h$ in general), the quality of service of the co-buyers. In addition, we use $f > 0$ to denote the "benefit" of sharing for friendship provided by the dishonest buyers. In contrast, f could also be regarded as the "cost" of the sharers from friendship sharing.

Consequently, without IBSPS, a user indexed by θ has a (total) utility function defined by

$$U_\theta = \begin{cases} \theta q_h - p, & \text{as an honest buyer,} \quad (12a) \\ \theta q_d - p + f, & \text{as a dishonest buyer,} \quad (12b) \\ \theta q_s - f, & \text{as a sharer,} \quad (12c) \\ \theta q_c - \frac{1}{2}p, & \text{as a co-buyer,} \quad (12d) \\ 0, & \text{if not using.} \quad (12e) \end{cases}$$

We assume that $f < q_s$, so that the user with the highest valuation for the service is better off becoming a sharer than not using the service (otherwise, friendship sharing would trivially not be an issue).

Based on the utility function, the following observations are pertinent:

- A buyer indexed by $\theta \geq p$ will intend to share the membership with friends if $q_h - q_d \leq \frac{f}{\theta}$. This inequality could be easily met based on the following two factors: one is the access portability which can help the users share the same membership efficiently, the other is that the sharing provider (i.e., the dishonest buyer) typically has higher priority than the sharing consumer (i.e., the sharer) to use the service. Both of these two factors could make the difference between q_h and q_d somehow trivial, such that sharing could be a better choice for the buyer.

- A potential consumer indexed by $\theta \geq p$ will be very happy to be a (free) sharer rather than a buyer or even a co-buyer whenever the sharing is possible and $q_h - q_s \leq \frac{p-f}{\theta}$ and $q_c - q_s \leq \frac{p-2f}{2\theta}$. The two inequalities could also be met if the quality of sharing is not so bad. Actually, because of the access portability of the digital subscription service, we can assume that there is not a big difference between q_h and q_s, as well as between q_c and q_s, and thus the inequalities hold. Such a kind of friendship sharing is exactly the main concern (worry) of the service provider.

- If it is not possible to find a "kind" sharing provider, or there is a big difference between q_c and q_s (i.e., $q_c - q_s > \frac{p-2f}{2\theta}$), a potential consumer indexed by $\theta \geq p$

may have another choice to enjoy the service, i.e., to buy it as a co-buyer rather than a buyer. This requires that $q_h - q_c \leq \frac{p}{2\theta}$. Although generally speaking, we can assume that $q_c \geq \frac{1}{2}q_h$[4], but when θ increases, a bigger q_c is also needed to satisfy the inequality condition. Combined with the possibility of friendship sharing, we argue that the joint-purchase is not very popular among the users with relatively higher valuations for the service.

- In contrast, a user indexed by $\theta < p$ will mostly choose joint-purchase if friendship sharing is not available and $q_c \geq \frac{p}{2\theta}$, i.e., joint-purchase is better off than not using. Since we assume that $q_c \geq \frac{1}{2}$ (suppose that $q_h = 1$) in general, the inequality requires that the value of θ is distributed on the interval $[\frac{1}{2}p, p)$ as for the case of 2-person joint-purchases[5]. It should be noted here that such kind of joint-purchases among the users with $\theta < p$ contribute extra revenue stream to the provider, since without joint-purchases those users would simply not buy the service.

If we consider the case with IBSPS, and let $\epsilon = \frac{1}{m} \cdot Z$ denotes the expectation value of prize for each buyer, the utility function for a user indexed by θ with IBSPS can then be revised as:

$$U^*_\theta = \begin{cases} \theta q_h - p^* + \epsilon, & \text{as an honest buyer,} \quad (13a) \\ \theta q_d - p^* + f, & \text{as a dishonest buyer,} \quad (13b) \\ \theta q_s - f + \epsilon, & \text{as a sharer,} \quad (13c) \\ \theta q_c - \frac{1}{2}p^* + \epsilon', & \text{as a co-buyer,} \quad (13d) \\ 0, & \text{if not using.} \quad (13e) \end{cases}$$

in which we assume that the above utility function adopts the revised IBSPS model proposed in Section 3.4, and $\epsilon' < \frac{1}{2}\epsilon$. Since with IBSPS, the service provider has to pay ϵ for each legitimate user, and thus the provider may somehow adjust the price to counterbalance the cost of ϵ and maximize its revenue. This is the reason that we use p^* to distinguish the price p defined in the utility function without IBSPS (see (12a) – (12d)). It should be noted that to achieve the maximal revenue, there is some relationship between p, p^*, and ϵ. We will further discuss this issue in the next section, and here we just simply assume that $p^* > p$ and $\epsilon > p^* - p$ in general.

Therefore, with IBSPS and the revised utility function, the users behaviors can be observed as follows:

- A buyer indexed by $\theta \geq p$ will not share anymore whenever $\epsilon \geq f - (q_h - q_d)\theta$. This inequality can be met by setting an appropriate ϵ for (most of) the buyers.

[4]Although the absolute value of usage time of each co-buyer is one half of that of an honest buyer, we could not simply say that the $q_c = \frac{1}{2}q_h$ since generally speaking, nobody would like to surf 24 hours a day. Due to the access portability, we assume that two co-buyers could negotiate together and find a solution to maximize each other's usage time pattern. In this case, we can assume that $q_c \geq \frac{1}{2}q_h$.

[5]As for n- person joint-purchases, the value of θ is distributed on $[\frac{1}{n}p, p)$.

- Suppose that the number of the dishonest buyers will decrease to some extent due to IBSPS, then the number of the sharers will also decrease simply because the sharing source is lost. Consequently, some of the users who cannot be the sharers anymore will choose to buy the subscription service by themselves as either a buyer or a co-buyer, and thus the total revenue of the producer will increase.

- The condition for a potential consumer who is indexed by $\theta \geq p$ and want to be a co-buyer rather than a buyer becomes stronger (more difficult) than that of without IBSPS, i.e, from $q_c \geq q_h - \frac{p}{2\theta}$ to $q_c \geq q_h - \frac{p^*}{2\theta} + \frac{\epsilon - \epsilon'}{\theta}$ (recall that $\epsilon' < \frac{1}{2}\epsilon$ and $\epsilon > p^* - p$).

More interestingly, since $\epsilon > p^* - p$, an honest buyer can actually enjoy more benefit (utility) with IBSPS. If an appropriate ϵ could be found to produce more revenue for the producers, then IBSPS can be served as a kind of win-win game for both of the consumers and producers. This is the issue that we will discuss in the next section.

5 Producer's Revenue Analysis with IBSPS

In IBSPS we assume that the producer must provide the money (prize) as the incentives to encourage the consumers to not share. A critical issue is that, how the producer can benefit from IBSPS by paying such an extra cost (of prize). Intuitively speaking, if the profits obtaining from the transformed new purchasers (i.e., the users who once were sharers or co-buyers but now have to or decide to buy the service by themselves in IBSPS) is higher than the cost of prize, then the producer can simply make more revenue back. In this section, we present a simple analysis about the revenue stream of the service producer with IBSPS as follows.

We start by considering a very simple market for an subscription service provided by a single producer. We assume there is a continuum of potential users who are characterized by their willingness to pay (valuation), θ, for the subscription service.

For clarity, we first model the n-person joint-purchase ($n \geq 2$) as a special kind of friendship sharing consisting of one representative (dishonest) buyer and $n-1$ (free) sharers. To this end, n co-buyers indexed by $\theta_1, \ldots, \theta_n$ ($\sum_{i=1}^{n} \theta_i \geq p$) is then transformed into one (representative) buyer indexed by $\theta_1' \geq p$, and $n-1$ sharers indexed by $\theta_2', \ldots, \theta_n'$, where $\sum_{j=1}^{n} \theta_j' = \sum_{i=1}^{n} \theta_i$. By means of such transformation, we can simplify the problem and consider only the case of friendship sharing in the subsequent analysis.

After the transformation, we assume that (the transformed) θ is still uniformly distributed on the interval $[0, 1]$. For each price p, the number of potential buyers with $\theta \geq p$ is $1 - p$. Suppose that without IBSPS, the ratio of the actual buyers to all the potential buyers with $\theta \geq p$ is fixed, say it is σ, and thus the numbers of the actual buyers and sharers with $\theta \geq p$ at price p are $\sigma(1-p)$ and $(1-\sigma)(1-p)$, respectively. Notice here we cannot say that the number of all the sharers with any θ is $(1-\sigma)(1-p)$, since there may be some transformed sharers (co-buyers) distributed on the interval $[0, p)$.

Without IBSPS, the producer's maximization program is then

$$\max_p \pi(p) = p \cdot \sigma(1-p) \tag{14}$$

The unconstrained profit-maximizing price and profits are easily computed as:

$$p_a = \frac{1}{2},\ \pi_a = \frac{\sigma}{4}$$

Suppose that with IBSPS, the producer provides a certain amount of prize Z for every m authorized buyers. Let $\epsilon = \frac{1}{m} \cdot Z$ denotes the expectation value of the prize for each buyer. We assume that with the expected prize ϵ, the ratio of the actual buyers to all the potential buyers at price p increases to σ' $(i.e., \sigma' \geq \sigma)$, and the numbers of the actual buyers and sharers with $\theta \geq p$ are $\sigma'(1-p)$ and $(1-\sigma')(1-p)$, respectively. Therefore, with IBSPS, the producer's maximization program becomes

$$\max_p \pi(p) = (p-\epsilon) \cdot \sigma'(1-p) \tag{15}$$

Here, the unconstrained profit-maximizing price is equal to

$$p_b = \frac{1+\epsilon}{2},\ \text{which implies } \pi_b = \frac{(1-\epsilon)^2\sigma'}{4}$$

This implies that to provide the expected prize ϵ to each authorized buyer with IBSPS, the producer has to increase the price at $\frac{1}{2}\epsilon$. It should be figured out that in (15) we assume that all the consumers are risk aversion. In other words, even the actual average price with IBSPS at price $p_b = \frac{1+\epsilon}{2}$ for each consumer is $\frac{1+\epsilon}{2} - \epsilon = \frac{1-\epsilon}{2}$, we assume that only those whose willingness to pay are greater than or equal to p_b will buy the service. This could be regarded as the worst case (assumption) for the producer to make profit with IBSPS.

To ensure the producer can profit from IBSPS, we have to guarantee that

$$\sigma' \geq \frac{1}{(1-\epsilon)^2}\sigma \tag{16}$$

Actually, the actual buyers at price p_b with IBSPS consists of two parts: one is those (original) buyers with $\theta \geq p_b$ at price p_a without IBSPS; the other is the (new) buyers changed from the sharers with $\theta \geq p_b$ (provided that some of the dishonest buyers will not share their memberships anymore due to IBSPS). We assume that with the expected prize ϵ, a certain percentage of buyers will not provide sharing anymore, say the percentage is a function over ϵ, say it is $\psi(\epsilon)$. We also assume that the willingness to pay of all the sharers are uniformly distributed on the interval $[0, 1]$. The ratio of the actual buyers to all the potential buyers with IBSPS can then be defined as follows:

$$\sigma' = \frac{1-\epsilon}{2} \cdot \sigma \cdot (1 + \psi(\epsilon) \cdot \frac{1-\sigma}{\sigma}) \tag{17}$$

Therefore, the producer can make profit with IBSPS if the following condition holds:

$$\psi(\epsilon) \geq \frac{2\sigma}{(1-\epsilon)^3 \cdot (1-\sigma)} - \frac{\sigma}{1-\sigma} \tag{18}$$

In practice, the goal of the producer is to find the smallest ϵ and the biggest $\psi(\epsilon)$ which satisfy (18), and thus to derive the highest π_b. However, to derive a realistic function of $\psi(\epsilon)$, we have to consider a variety of socioeconomic factors depending on different prices and services. Since we cannot do that without a comprehensive empirical and theoretical study, we do not further analyze it in this article and leave it as an open issue.

6 Concluding Remarks

In this article, we first presented an analysis on membership sharing problem in digital subscription services, and then proposed an incentives-based secrets protection system (IBSPS) to solve the problem.

The idea of IBSPS is originally inspired by SPIES (Secret Protection Incentive-based Escrow System) [9] (Margolin et al., 2004), which aims to provide an economic negative incentive to not sell secrets so as to make profit. The main idea of SPIES is to require a consumer to place an amount of additional security deposit — which is typically several times than the price of the secret per se — into a trusted escrow account beforehand, and the consumer will totally lose some deposit whenever unauthorized reselling happens because everyone who knows the secret can register to the escrow and "steal" a part of the deposit away.

An important assumption of SPIES is that it assumes that concurrent access with the same secret (account) is not technically prohibited, but the provider can somehow detect the concurrent usage and thus deactive the account afterwards. Suppose there is some number of users at which it becomes trivially obvious to the provider that more than one user is accessing the account, say the number is n, the required deposit is then set to $v = (n + 1)p$ (where p is the price of the service), such that an authorized user can never resell the account to more than n rational people so as to make profit. In this case, if $n \leq 2$ then SPIES is unnecessary as stated in [9]. In other words, if concurrent access is technically explicitly prohibited, then SPIES is also unnecessary.

More importantly, the deposit idea of SPIES cannot solve the sharing problem among friends, while it is somewhat useful to solve the sharing problem caused by reselling to strangers. This is because everyone who knows the secret can receive a part of the deposit with one hundred percent, and thus it becomes trivially obvious to the sharing provider (called as dishonest buyer or co-buyer in IBSPS) that some friends have stolen his deposit once he cannot receive the whole deposit back. To this end, the sharing consumers (called as sharers or co-buyers in IBSPS) may not take the risk to register to the escrow secretly, since such kind of betraying is easy to be disclosed, especially in the case of 2-person sharing. However, with the lottery idea of IBSPS, i.e., everyone is possible to get the prize but no one with a hundred percent, the sharing problem among friends can be somewhat handled because now it becomes the sharing provider's worry that his friends may steal his money (expected prize) without his knowledge. For a more detailed comparison between IBSPS and SPIES, we refer to [17].

It should be noted that in IBSPS, we assume that the service provider has no incentive to share the membership with unauthorized users, and the provider is trustable and

will not take part in the lottery even it knows all the secrets of the users. If the provider is not trustable, for example, suppose that the provider want to grab some prize back secretly, then additional mechanism should be added so as to protect the interest of the honest buyers. This is somehow a different problem, and it is also one of our future directions.

An interesting issue about sharing is that whether sharing should be prevented or even "encouraged" with respect to different digital contents and subscription services. For instance, sharing music with friends is one of the main ways that people find out about new music, and thus it could be more useful for DRM systems to concentrate on how sharing and exploring new music can leat to a purchase, rather than try to stop a core music activity, i.e., sharing [7]. This conjecture somehow holds because there is some relationship between listening and buying, and people usually enjoy their favorite music for many times. But, how about movies, online magazines, and other digital contents? For instance, how many people would like to buy the DVDs (physical magazines) after they have already watched the movies (magazines) on line? From this point of view, sharing is still a problem as for most of the digital contents and subscription services.

Unlike sharing among friends, IBSPS may fail with respect to sharing among family, since generally speaking there is no incentive for a family member to "steal" the money from another family member. The sharing among family could be regarded as a special kind of joint-purchase, especially when the family members actually have similar interests.

The key practical issue of IBSPS for the producer is to determine σ (i.e., the ratio of actual buyers to all the potential buyers whose willingness to pay is greater than the price), and then to find an appropriate function of $\psi(\epsilon)$ so as to get the maximal revenue π_b. Although generally speaking, the value of σ without IBSPS is difficult to know, it can be appropriately estimated based on the number of multiple registrations with the same secrets with IBSPS, i.e., a kind of posterior parameter. In addition, $\psi(\epsilon)$ is also a kind of posterior function whose accurate value can only be determined by comparing the the results without and with IBSPS. Moreover, the value of $\psi(\epsilon)$ may vary as for different applications and prices of the services, that is the reason that we leave it as an open issue as mentioned at the end of the last section.

7 Acknowledgements

We gratefully acknowledge our discussions with Prof. Dines Bjørner and Prof. René Vestergaard of Japan Advanced Institute of Science and Technology, especially for the their valuable comments on possible biometric authentication techniques for DRM and formal game theory, respectively.

This research is supported by 21st COE (Center of Excellence) Program "Verifiable and Evolvable e-Society" of JAIST, a funds by Ministry of Education, Culture, Sports, Science and Technology (MEXT, Japan). It is also conducted as a program for the "Fostering Talent in Emergent Research Fields" in Special Coordination Funds for Promoting Science and Technology by MEXT of Japan.

References

[1] Feng Bao, Robert H. Deng, and Wenbo Mao. Efficient and practical fair exchange protocols with off-line ttp. In *Proceedings of 1998 IEEE Symposium on Security and Privacy*, pages 77–85, Oakland, CA, 1998. IEEE Computer Society.

[2] J. G. Cosgrove and P. B. Linhart. Customer choices under local measuered telephone service. *Public Utilities Fortnightly*, pages 27–31, Aug. 30 1979.

[3] Marc Fetscherin and Matthias Schmid. The application of digital rights management systems in the music industry – an empirical investigation. In *Proc. of the Third International Conference WEB Delivering of Music (WEDELMUSIC'03)*. IEEE, 2003.

[4] Peter Fishburn, Andrew M. Odlyzko, and Ryan C. Siders. Fixed fee versus unit pricing for information goods: Competition, equilibria, and price wars. *First Monday*, 2(7), July 1997.

[5] L. Garfinkel and P. B. Linhart. The transition to local measured telephone service. *Public Utilities Fortnightly*, pages 17–21, Aug. 16 1979.

[6] L. Garfinkel and P. B. Linhart. The revenue analysis of local measured telephone service. *Public Utilities Fortnightly*, pages 15–21, Oct. 9 1980.

[7] Margaret Jackson, Supriya Singh, and Jenny Waycott. DRMs, fair use and user's experience of shairng music. In *DRM'05*, pages 8–16, Alexandria, Virginia, USA, Nov 2005. ACM.

[8] Salvador Mandujano and Rogelio Soto. Deterring password sharing: user authentication via fuzzy c-means clustering applied to keystroke biometric data. In *Proceedings of the Fifth Mexican International Conference in Computer Science, ENC 2004*, pages 181–187. IEEE, 2004.

[9] N. Boris Margolin, Matthew K. Wright, and Brian N. Levine. Analysis of an incentive-based secrets protection system. In *Proc. of the 4th Internation Workshop on Digital Rights Management*, pages 22–30, Washing, DC, USA, Oct 2004. ACM.

[10] B. M. Mitchell and I. Vogelsang. *Telecommunications Pricing: Theory and Practice*. Cambridge Univ. Press, 1991.

[11] Deirdre K. Mulligan, John Han, and Aaron J. Burstein. How drm-based content delivery systems disrupt expectations of "personal use". In *Proc. of The 3rd International Workshop on Digital Rights Management*, pages 77–89, Washington DC, USA, Oct 2003. ACM.

[12] MusicAlly. Napster users sharing passwords to save cash, Apr 8th 2005. http://www.theregister.co.uk/2005/04/08/napster_password_sharing/.

[13] M. Mussa and S. Rosen. Monopoly and product quality. *Journal of Economic Theory*, 18:301–317, 1978.

[14] Commission of The European Communities. Digital rights: Background, systems, assessment. Commission Staff Working Paper, 2002. Brussels, 14.02.2002, SEC(2002) 197.

[15] Stéphane Le Roux, Pierre lescanne, and René Vestergaard. A discrete nash theorem with quadratic complexity and dynamic equilibria. Technical Report JAIST/IS-RR-2006-006, Japan Advanced Instiute of Science and Technology, Asahidai 1-1, Nomi, Ishikawa, 923-1292 Japan, 2006.

[16] Carl Shapiro and Hal Varian. *Information Rules: A Strategic Guide to the Network Economy*. Harvard Business School Press, Boston, Massachusetts, 1998.

[17] Jianwen Xiang, Weiqiang Kong, Kokichi Futatsugi, and Kazuhiro Ogata. Analysis of positive incentives for protecting secrets in digital rights management. In José Cordeiro, Vitor Pedrosa, Bruno Encarnaç ao, and Joaquim Filipe, editors, *Proc. of the Second International Conference on Web Information Systems and Technologies (WEBIST'06)*, Setúbal, Portugal, April 2006. INSTICC, INSTICC Press.

[18] Yong-Bin Zhou, Zhen-Feng Zhang, Si-Han Qing, and Juan Liu. A new cembs based on rsa signatures and its application in constructing fair exchange protocol. In *Proceedings of The 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'04)*, pages 1–5. IEEE Computer Society, 2004.