Presented at 8th International Conference of the Society for Computational Economics

(Aix en Provence, France, June 2002)

Digital Security Tokens in Network Commerce: Modeling and Derivative Application

Kanta Matsuura*

Institute of Industrial Science, University of Tokyo (Japan)

Abstract

Digital objects in network commerce cause new credit risks (*e.g.* by an unpredictable compromise of a secret key and the resultant revocation of the corresponding public-key certificate). We recognize that we need to study a new financial risk management in this respect. The study firstly needs models. This paper describes a full framework of modeling uncertain digital objects distributed in a network society. We have made an abstraction of the objects and defined "security token", which is abbreviated into a word coinage *setok*. Each setok has its price, values, and timestamp on it as well as the main contents. Not only the price but also the values can be uncertain and may cause risks. A number of properties of the setok are defined. They include value response to compromise, price response to compromise, refundability, tradability, online divisibility, and offline divisibility. Then a derivative written not on the price but on the value is introduced. With the help of popular stochastic theory, we derive several option-pricing formulae. These formulae do not require any divisibility of the underlying setok.

In search of applications, an inverse estimation of compromise probability is studied. We derive a partial differential equation (PDE) to price a call option; given a set of parameters including the compromise probability, the PDE can tell us the option price. By making an inverse use of this, we can estimate the risk of compromise.

In addition to related works and future directions, a comprehensive discussion on the relation between information-security technologies and economics is given. The discussion also shows how financial tools can help information security in the real world, and thus enriches the implications of this framework.

Key words: network commerce, information security, public-key certificate, trust, setok, option pricing, credit risk.

* *Correspondence to:* Dr. K. Matsuura, Institute of Industrial Science, University of Tokyo, Komaba 4-6-1, Meguro-ku, Tokyo 153-8505, JAPAN. Tel. +81-3-5452-6284, Fax.: +81-3-5452-6285, E-mail: kanta@iis.u-tokyo.ac.jp

Contents

1 Introduction

Applied cryptography[1] opens a door to a market of digital products in a network society. With the help of advertisement attached, the products do not necessarily have positive prices; they can be free of charge. In this case, the recipients may no longer think of them as products. So we will use the phrase *digital objects*, instead of digital products, in the following.

Since digital data in general can keep their original bit strings virtually forever, one may expect that there would be no risk of change in qualities of digital objects. This is, unfortunately, not the case.

In addition to the prices, digital objects likely have other numerical values. For example, digital images and multimedia contents may have popularity indices. Their qualities may be controlled by copyright protection mechanisms[2], [3], and hence they may have quality labels and usage-restriction numbers. Multi-purpose tokens may have reward points which would expire someday. Any object may be associated with an insurance contract stating how much will be paid in the case of a significant damage to the object [4]. If the use of the objects needs access-grant tickets, they may have priority numbers or QoS (Quality-of-Service) values reserved [5]–[8]. The functions mentioned above are typically achieved by using digital signatures whose trustworthiness is resorted to digital certificates, and the certificates themselves may be combined with confidence values [9]–[12]. These additional values may change unpredictably over time and cause risks.

Let us see a simple example. Suppose that you buy a digital ticket issued and digitally signed by an issuer. The ticket can be used for a remote-access service. On purchase, you of course verify the digital signature. Signature verification procedure includes verification of a certificate associated with the public key of the signer. It fortunately succeeds. On the next day, you make an attempt to use the ticket. The remote-access server verifies the issuer's signature on your ticket. Unfortunately, the public-key certificate of the issuer is turned out to have been revoked due to an unexpected event, and therefore the verification fails. You can no longer use your ticket[1].

This risk may be recognized as a new type of *credit risk*[13], [14] specific to network economics based on information-security technologies. We need appropriate risk management theories, and firstly theories need models; we have to identify what are primary features of the digital objects distributed in the society. The first report of this identification and possible application of it was given in [15]. However, it was unfortunately in its infancy. The purpose of this paper is to show the full framework on this identification, and then to develop a basic theory of derivatives in the model identified. From the engineering point of view, we also explore applications of the framework. Different from the corresponding theory and application in [15], this paper enriches their implications significantly: more generalizations, deeper interpretations, surveys of related areas, and a comprehensive discussion on the relation between information-security technologies and economics.

Specifically, the paper is organized as follows. First, in Section 2, we model uncertain digital objects as a *security token*, which will be abbreviated into a word coinage ***setok*** in contrast to an existing word *stock*. Written on a tradable setok, a European call option

[1] This is a *simple* example because, in general, we can have a trust metric computed from a set of certificates. A revocation does not always imply a complete default of the certificate set.

is defined and priced in Section 3, where discrete-time models are firstly studied. The last part of Section 3 deals with a continuous-time model. By using a well-known lemma in stochastic calculus, an option-pricing formula is derived. A numerical analysis of the formula is provided as well. We then explore an application of option pricing in Section 4: inverse estimation of compromise probability. After a survey of related works in Section 5, Section 6 concludes the paper with indicating future directions. The survey includes a relation between this work and credit derivatives. A comprehensive discussion on the relation between information/network security and economics is included there as well.

2 Security Token

2.1 Network Society

We start with our basic architecture of the network commerce, which is illustrated in Fig. 1.

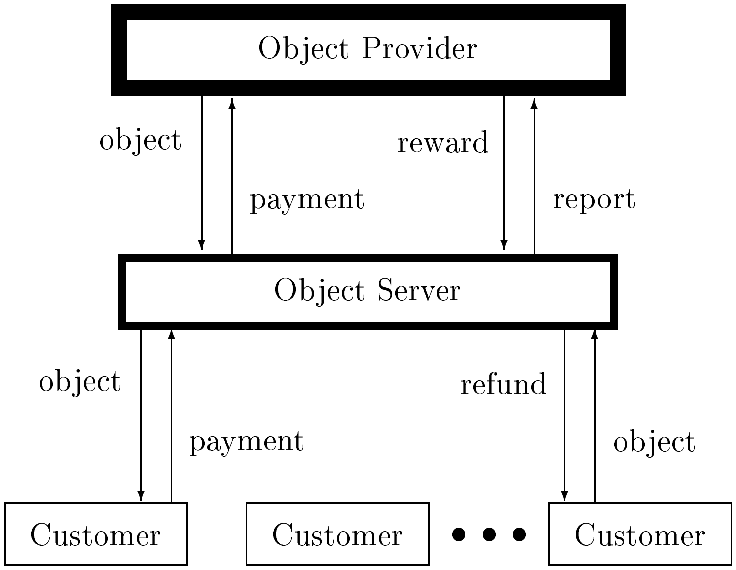

Figure 1: Basic architecture of the network commerce. Boxes with wider lines indicate that the entities inside are more trusted. The object provider and server are able to keep in touch with the up-to-date market information. Some customers are able to keep in touch with the up-to-date market information but the others are not. Due to better reputation and/or advertisement profits, the provider would be happier if the objects are distributed and circulated more frequently in larger amounts. The refund may depend on the price and/or values of the object. The payment from a customer may be regarded as a deposit, depending on the situation; this architecture can model a rental system as well. Basically, each payment is made by digital cash.

The observation to have this architecture is as follows:

(Object Provider) For example, copyright management and related technical maintenance are not easy and trivial tasks with respect to digital objects. Management and maintenance of network-security infrastructure (*e.g.* public-key infrastructure) are not, either. These tasks may require sufficient trustworthiness and reliability. We need specialized entities which are eligible for them. Typically, they are trusted organizations or licensed firms. Object providers would be happier if the objects they provide are distributed and circulated more frequently in larger amounts; it would improve their reputation and/or make attached advertisement more profitable. They would have a motivation to give rewards for active usage of the objects. They are able to keep in touch with the up-to-date market information.

(Customer) We do not trust individuals in terms of (i) their own behaviour, (ii) their financial situation, and (iii) resources (for communication and computation) available to them. Some customers are able to keep in touch with the up-to-date market information but the others are not. In terms of trading amount, the former would be the major contributors. Since we allow untrusted individuals, the system can be *ubiquitous:* many people can enjoy transactions in various situations including mobile settings.

(Object Server) Selling digital objects to distrusted customers is another difficult and non-trivial task. We need specialized entities which can do it and have a good connection with object providers. Typically, they are trusted organizations or firms; they can be less trusted in comparison with object providers but they must be more trusted than customers. Due to the rewards from object providers as well as their basic business reasons, object servers would like to enhance their trading activities with customers. One may think that it is easy to sell more because copying digital data in general is so easy. However, as already implied, this is not true for digital objects; if the object providers work well, they are the only entities who can increase the number of the objects either by copying or by creating a new version. Thus object servers would have a motivation to re-circulate the objects. They may be able to get the objects back from their customers in exchange for some refund. The refund may depend on the price and/or values of the object. Object servers are able to keep in touch with the up-to-date market information.

The observation above is very important in view of forthcoming derivative studies because how to specify observability often constitutes a core part of credit-derivative pricing[16].

2.2 Setok

Based on the basic architecture, we model uncertain digital objects as follows.

Definition 2.1 (Setok) *A* **security token** *or* **setok** *is a digital material which* **nominally contains** *the following four attributes:*

- **contents** *which may include MAC (Message Authentication Code), digital signatures, or other security-related control sequences if necessary,*

- *a non-negative* **explicit price** *(denoted by $\bar{S}$) which is paid when the setok is purchased by a customer,*

- *a set of non-negative* **explicit values** *(denoted by $\bar{V_1}$, $\bar{V_2}$, $\cdots$, $\bar{V_m}$ where m is referred to as the* **dimension** *of the explicit values) which represent some qualities of the contents in a way that larger values of each element imply better qualities regarding the feature represented by the element when the setok is purchased, and*

- *a* **timestamp** *which indicates when the setok is purchased,*

and is associated with

- *a non-negative* **implicit price** *(denoted by S) and*

- *a set of non-negative* **implicit values** *(denoted by V_1, V_2, $\cdots$, V_n where n is referred to as the* **dimension** *of the implicit values)*

in the following way.

- *The explicit price is specified as the occurrence of a* **price-interpretation process** $Y(t){=}y\,(t, S\,(t))$*;* i.e. *the specific numerical value $y\,(t_0, S\,(t_0))$ is written as the explicit price of the setok which is purchased at time $t = t_0$. Each occurrence of the price-interpretation process is called the* **up-to-date price** *at time t. The price-interpretation process is a non-negative process and also called the* **up-to-date price process**. *$y(t, s)$ is called a* **price-interpretation function** *and monotone increasing with respect to s. Customers are unable to change the explicit price.*

- *The explicit values are specified as the occurrences of* **value-interpretation processes** $H_1(t){=}h_1(t,\ V_1(t),\ V_2(t),\ \cdots,\ V_n(t))$, $H_2(t){=}h_2(t,\ V_1(t),\ V_2(t),\ \cdots,\ V_n(t))$, $\cdots$, $H_m(t){=}h_m(t,\ V_1(t),\ V_2(t),\ \cdots,\ V_n(t))$*;* i.e. *the specific numerical value $h_i(t_0,\ V_1(t_0),\ V_2(t_0),\ \cdots,\ V_n(t_0))$ is written as the i-th explicit value of the setok which is purchased at time $t = t_0$ (i = 1, 2, $\cdots$, m). Each occurrence $h_i(t,\ V_1(t),\ V_2(t),\ \cdots,\ V_n(t))$ is called the i-th* **up-to-date value** *at time t. The value-interpretation processes are non-negative processes, and also called the* **up-to-date value processes**. *$h_1(t,\ v_1,\ v_2,\ \cdots,\ v_n)$, $h_2(t,\ v_1,\ v_2,\ \cdots,\ v_n)$, $\cdots$, $h_m(t,\ v_1,\ v_2,\ \cdots,\ v_n)$ are called* **value-interpretation functions**. *Customers are unable to change the explicit values.*

When we say "*security* token", we consider three notions at the same time:

1. *Information security* such as confidentiality, authenticity, integrity, non-repudiation, and availability.

2. *Official* pieces of writing, *e.g.* bonds and stocks.

3. What gives the owner the *right* to certain property.

Definition 2.1 accepts not only purely financial digital materials but also digital commodities as setoks; we have not specified the contents.

Customers are distrusted. Depending on the payment scheme, customers may be even anonymous when they buy setoks. So each payment must be settled on site in exchange of the corresponding pieces of the setok. This should be done in a secure way; no customer can exploit a setok without payment, and no server can exploit a payment without sending the setok. Servers are trusted but we do not want to allow customers to lay frame-up accusation against servers. Thus setoks are transmitted to customers in pieces; *e.g.* "three pieces" are possible but "two and a half pieces" are impossible. A piece of setok will be referred to as a **share** of the setok.

A setok in the market is denoted by $(S;\ Y;\ V_1,\ V_2,\ \cdots,\ V_n;\ H_1,\ H_2,\ \cdots,\ H_m)$ or sometimes shorthandly by $(S,\ Y;\ V,\ H,\ n,\ m)$. Likewise, a share of the setok already purchased and held by someone is denoted by $(\bar{S};\ \bar{V}_1,\ \bar{V}_2,\ \cdots,\ \bar{V}_m;\ t_0)$ or sometimes shorthandly by $(\bar{S};\ \bar{V},\ m;\ t_0)$.

The price-interpretation function can model the effect of taxes, transaction costs, regulatory issues, and so on. The value-interpretation functions can model the effect of security policies, regulatory issues, editorial policies, transmission delay, and so on. Suppose that we make an electronic version of a stock in a way that each share of the setok has the explicit values which tell the firm's information evaluated somehow. The "evaluation" or "interpretation" may include an *editorial* process or *aggregation* procedures. It is impractical to write every history of the firm on a setok, even though it is a digital material.

It should be noted that we have *not* mentioned any increasing or decreasing properties of the value-interpretation functions. A tricky but efficiently implementable example is a one-way hash function. Even when we have implicit values which are extremely large in size (number of bits), hashed values can be in a practical size. This example might remind us of a gamble; the explicit values, which are completely unpredictable in advance, represent yet some qualities of the material in a way that larger values of each element imply better qualities. The implicit values do not necessarily represent such qualities; they cause fluctuation.

The "up-to-date" processes, $Y(t)$ and $H(t)$, are observable in the market and hence are adapted processes. Note that

- some of the implicit processes $S(t),\ V_1(t),\ V_2(t),\ \cdots,\ V_n(t)$ may be **not** adapted processes **even if**
  - the explicit value is one-dimensional (*i.e.* $m = 1$),
  - both of the price/value interpretation functions are easy to compute, and strictly monotone increasing functions with respect to some implicit price or implicit values, and
  - the other implicit price/value processes are adapted processes.

For not strictly monotone increasing functions, we may easily accept the note above. The following is a trivial example:

Example 2.1 *Let us consider a setok* $(S, Y; V, H, n, 1)$ *with a price-interpretation function* $y(t, s) = s$ *and a value-interpretation function* $h_1(t,\ v_1,\ v_2,\ \cdots,\ v_n)= h_0$ *where* h_0 *is a deterministic constant.* y *is strictly monotone increasing with respect to* s *but* h_1 *is not strictly monotone increasing with respect to any* v_j*. The implicit price process is an adapted process but the implicit value processes are not.*

However, at a first glance, it would be more difficult or counter-intuitive, especially for those who are unfamiliar with information-security engineering, to see that strictly monotone increasing interpretation functions do not always guarantee the adaptation. We demonstrate it by using a one-way hash function.

Example 2.2 *Let us consider a setok* $(S, Y; V, H, 2, 1)$ *with a price-interpretation function* $y(t, s) = s$ *and a value-interpretation function*

$$h_1(t, v_1, v_2) = h(v_2) + p \cdot v_1$$

where $h(\cdot) : \boldsymbol{N} \to \boldsymbol{Z}_p$ *is a one-way hash function,* $\boldsymbol{N} = \{1, 2, 3, \cdots\}$ *is the set of positive integers,* $\boldsymbol{Z}_p$=$\{0, 1, 2, \cdots, p-1\}$*, and* p *is a large positive integer (constant). Let us suppose* $V_1(t) \in \{0, 1\}$*,* $V_2(t) \in \boldsymbol{N}$ *for any* $t \in \boldsymbol{T}$*. Then* y *is strictly monotone increasing with respect to* s*, and* h_1 *is strictly monotone increasing with respect to* v_1*. The implicit price process is an adapted process.* V_1 *is also an adapted process because* $H_1(t) \geq p$ *implies* $V_1(t) = 1$ *and* $H_1(t) < p$ *implies* $V_1(t) = 0$*. Nevertheless,* V_2 *is not an adapted process.*

Remark 2.1 *Regarding stochastic variables, we follow the conventions in notation:*

- *Stochastic variables often appear with suppression in the following part of the paper;* e.g. *for readability reasons, we would write* S *instead of* $S(t)$ *nor* $S(t)[\omega]$ *where* $\omega \in \Omega$ *and* Ω *is the universe of the probability space considered.*
- *(1) An occurrence of a stochastic variable, and (2) corresponding arguments in functions describing other processes by the use of the stochastic variable, are usually written in small letters.*

2.3 Price and Value

Recall that sufficient information to determine the implicit price and values is not necessarily obtained through market observation, although the up-to-date price and values are observable in the market. Let us consider in more detail about the relationship or correlation among the implicit/up-to-date price and values.

The explicit values represent some qualities of the setok. They depend on the implicit values. The bridge between them is the value-interpretation functions. Changes in the implicit values may be relaxed through the interpretation. They may be exaggerated, too.

Let us suppose a value-interpretation function h_i which is monotone increasing with respect to the j-th implicit value. In this case, intuitively, the implicit value V_j also represents some sort of quality of the material. Let us suppose that some sort of *compromise* has just reduced the j-th implicit value to be zero. Hopefully best efforts are made to make the up-to-date values reflect this emergency well enough. The efforts may include, for example, implementing the underlying directory system with real-time *revocation* as well as periodical/regular update[2]. From the viewpoint of setok, an ideal situation is defined as follows.

Definition 2.2 (Value Response to Compromise) *Let a setok $(S, Y; V, H, n, m)$ have one or more value-interpretation functions which are monotone increasing with respect to one or more implicit values. Let $\{V_{j_1}, V_{j_2}, \cdots, V_{j_s}\}$ be the set of all such implicit value processes.*

Then, the setok is said to be **compromised** *if and only if $V_{j_1}(t){=}V_{j_2}(t){=}\cdots{=}V_{j_s}(t) = 0$. This setok is said to be* **compromise-responsive in value** *if and only if the following condition is satisfied.*

- *For any h_i which is monotone increasing with respect to one or more implicit values $V_{j_1}, V_{j_2}, \cdots, V_{j_s}$, a compromise $V_{j_1}(t){=}V_{j_2}(t){=}\cdots{=}V_{j_s}(t) = 0$ implies $H_i(t) = 0$. When $H_i(t)$ becomes zero, the setok is said to be* **revoked** *with respect to the i-th up-to-date value.*

Do you accept a positive price for a “compromised” material? The answer may be not unique and depend on the relationship between the contents and the implicit/explicit values. We shall define a special, but easier to accept, situation.

Definition 2.3 (Price Response to Compromise) *Let a setok $(S, Y; V, H, n, m)$ have one or more value-interpretation functions which are monotone increasing with respect to one or more implicit values. Let $\{V_{j_1}, V_{j_2}, \cdots, V_{j_s}\}$ be the set of all such implicit value processes.*

This setok is said to be **compromise-responsive in price** *if and only if the compromise $V_{j_1}(t){=}V_{j_2}(t){=}\cdots{=}V_{j_s}(t) = 0$ implies $Y(t) = 0$.*

2.4 Resale of Setoks

Object servers have a motivation to re-circulate the objects they have sold. They may be able to get the objects back from their customers in exchange for some refund, which would in turn motivate the customers to return the objects. This refund may depend on the price and/or values of the object. Formally, we define refundability and tradability.

---

[2] In this context, the compromise is a primary disaster and the revocation is a response to it.

Definition 2.4 (Refundability) *A share of setok is said to be* $\boldsymbol{T}$**-refundable** *if and only if the following two conditions are satisfied:*

- *The explicit price is positive.*
- *The holder can sell it whenever he wants during a set of time intervals* $\boldsymbol{T}$*,* i.e. *at any time* $t \in \boldsymbol{T}$*, at the price of the explicit price.*

$\boldsymbol{T}$ *is called a* **refundable period** *and allowed to be composed of open and closed time intervals; all of the forms* $[T_L, T_U]$*,* $[T_L, T_U)$*,* $(T_L, T_U]$*, and* (T_L, T_U) *(and set of them) are available. The refundable period can be either deterministic or stochastic. When the context does not need the refundable period, we can just say "refundable" instead of "*$\boldsymbol{T}$*-refundable".*

In particular, a share of setok is said to be ∞**-refundable** *if and only if it is* $[t_0, \infty)$*-refundable where* t_0 *is the timestamp on it.*

Definition 2.5 (Strict Refundability) *A share of setok is said to be* **strictly** $\boldsymbol{T}$**-refundable** *if and only if the following three conditions are satisfied:*

- *It is* $\boldsymbol{T}$*-refundable.*
- *The refundable period* $\boldsymbol{T}$ *is deterministic.*
- *The holder cannot sell it at any price when it is out of the refundable period* $\boldsymbol{T}$*.*

When the context does not need the refundable period, we can just say "strictly refundable" instead of "strictly $\boldsymbol{T}$*-refundable".*

In particular, a strictly $\emptyset$*-refundable setok is said to be* **unrefundable** *where* $\emptyset$ *is the empty set.*

Definition 2.6 *At time* t*, a strictly* $\boldsymbol{T}$*-refundable setok with non-empty refundable period* $\boldsymbol{T}$ *is said to be* **still refundable** *if and only if there exists a time* t' *such that* $t' > t$ *and* $t' \in \boldsymbol{T}$ *where* t *is the current time.*

There are several important things to be pointed out. Firstly, note that we have defined the refundability with respect to a *share* of setok. Even for the same setok, shares sold at different time could have different refundable periods; the refundability of ($\bar{S}$; $\bar{V}$, m; t_0) and that of ($\bar{S}$; $\bar{V}$, m; t_1) ($t_1 \neq t_0$) are not necessarily the same. This allows a dynamic change of management policies of a setok. For example, let us suppose a setok which has been managed so far in a way that all the shares are strictly refundable and the refundable period is very long. This policy gives an assurance to customers, but could cause too much financial load (*e.g.* reserve funds) on the server and/or too much administrative load (*e.g.* security-parameter directory) on the provider. If needed, the policy can be changed in a way that shares will be sold with a shorter refundable period, or even sold with no refundability, from now on. However, due to the former strict refundability, the refundable periods of the shares already sold cannot be changed accordingly. If their refundable periods were stochastic, the corresponding change would be (not mandatory but) possible. Thus, in our framework, we can accommodate a wide variety of situations by specifying which kind of refundability is used.

It should be also noted that the refund of a setok is possible only at its explicit price $\bar{S}$. Changes in values are not considered. This can model a rental system with deposit, for example. However, depending on the applications, a more flexible resale may be allowed. This is easier if the explicit value is one-dimensional.

Definition 2.7 (Single-Valued Setok) *A setok is said to be* **single-valued** *if and only if it has one-dimensional* explicit *value. In the case of a single-valued setok, we often omit the subscript "1" when we denote the explicit value, the corresponding value-interpretation function, and the corresponding value-interpretation process. Hence we may write*

$$\bar{V} = H(t_0) = h(t_0, V_1(t_0), V_2(t_0), \cdots, V_n(t_0)).$$

Definition 2.8 (Tradability) *A share of single-valued setok is said to be* $\boldsymbol{T}$**-tradable** *if and only if the following two conditions are satisfied:*

- *The explicit value $\bar{V}$ is positive.*
- *Whenever he wishes during a set of time intervals $\boldsymbol{T}$,* i.e. *at any time $t \in \boldsymbol{T}$, the value-interpretation process is positive and the holder of the setok can sell it. This resale is possible only at the* **value-proportional price** *S_p defined by*

$$S_p = \frac{\bar{V}}{h(t, V_1(t), V_2(t), \cdots, V_n(t))} y\left(t, S\left(t\right)\right).$$

$\boldsymbol{T}$ *is called a* **tradable period** *and allowed to be composed of open and closed time intervals; all of the forms $[T_L, T_U]$, $[T_L, T_U)$, $(T_L, T_U]$, and (T_L, T_U) (and a set of them) are available. The tradable period can be either deterministic or stochastic.*

In particular, a setok is said to be ∞-**tradable** *if and only if it is $[t_0, \infty)$-tradable where t_0 is the timestamp on it.*

Lemma 2.1 *The value-proportional price S_p is a non-negative adapted process.*

Proof : Trivial from Definition 2.8. ***Q.E.D.***

It should be noted here that S_p can have a zero occurrence; there can be a trade at a price of zero.

One may wonder why we restrict the trading to the value-proportional price; there might be a case in which the mapping from the space of (time, implicit values, explicit value, implicit price) to the space of trading price takes a more complicated form. Our answer to this question is that we model the complexity in terms of value-interpretation functions.

Definition 2.9 (Strict Tradability) *A setok is said to be* **strictly $\boldsymbol{T}$-tradable** *if and only if the following three conditions are satisfied:*

- *The setok is $\boldsymbol{T}$-tradable.*
- *The tradable period $\boldsymbol{T}$ is deterministic.*
- *The holder of it cannot sell it at any price when it is out of the tradable period $\boldsymbol{T}$.*

In particular, a strictly $\emptyset$-tradable setok is said to be **untradable** *where $\emptyset$ is the empty set.*

Definition 2.10 *A strictly $\boldsymbol{T}$-tradable setok with non-empty tradable period $\boldsymbol{T}$ is said to be* **still tradable** *if and only if there exists a time t' such that $t' > t$ and $t' \in \boldsymbol{T}$ where t is the current time.*

2.5 Divisibility

Tradability and refundability do not cover all the flexibility concerns about setoks. Suppose a situation in which I need a single-valued setok $(S, Y; V, H, 1, 1)$ with an explicit value of 100. And suppose that I am so unlucky that the current market board says $H(t) = 95$. Shall I buy two shares of the setok? Do I have to reconsider my purchase plan? This annoyance depends on the divisibility of the setok.

Definition 2.11 (Online Divisibility) *A setok $(S, Y; V, H, n, m)$ is said to be* **online-divisible** *if and only if the following condition is satisfied.*

- *Whenever the occurrence of the price-interpretation process is positive, anyone can purchase an arbitrary fraction of the setok with keeping* **proportional explicit values***;* i.e. *at an arbitrary* **order price** *$S_c > 0$, he can buy the setok at the explicit price S_c and explicit values*

$$\frac{S_c}{Y(t_0)} h_i(t_0, V_1(t_0), V_2(t_0), \cdots, V_n(t_0)) \ (i = 1, 2, \cdots, m)$$

assigned where t_0 is the timestamp on it.

It should be noted here that we make an order by specifying the order price, not by specifying the explicit values. This can decrease communication overhead.

We may face a similar annoyance when we are going to sell a share of setok.

Definition 2.12 (Offline Divisibility) *A share of setok* $(\bar{S}; \bar{V}_1, \bar{V}_2, \cdots, \bar{V}_m; t_0)$ *which has a positive explicit price* $\bar{S}$ *is said to be* **offline-divisible** *if and only if the holder of it can divide it into two pieces,* $(\bar{S}^1; \bar{V}_1^1, \bar{V}_2^1, \cdots, \bar{V}_m^1; t_0)$ *and* $(\bar{S}^2; \bar{V}_1^2, \bar{V}_2^2, \cdots, \bar{V}_m^2; t_0)$*, in a* **price-proportional manner***,* i.e.

$$\bar{S}^1 + \bar{S}^2 = \bar{S},\ \bar{S}^1 > 0,\ \bar{S}^2 > 0$$

and

$$\bar{V}_j^i = \frac{\bar{S}^i}{\bar{S}} \bar{V}_j,\ (i = 1, 2; j = 1, 2, \cdots, m).$$

One may wonder why we have define not only the online divisibility but also the offline divisibility. This distinction is needed to enrich the variety of flexibilities. In the setok world, entities or agents live under uncertainty. Even if all the exogenous stochastic dynamics are given, their optimal strategies depend on the divisibilities in a different manner; roughly speaking, the online divisibility contributes to the flexibility of purchase whereas the offline divisibility contributes to the flexibility of resale and subsequent investments. So the online divisibility is defined with respect to a setok whereas the offline divisibility is defined with respect to a *share* of setok.

One may also wonder why we have paid so much attention to divisibility in a digital world, by saying “It is very easy to divide digital data, isn’t it? That should be a virtue of computers and computer networks!” Unfortunately, this is not the case in general. Our experiences in applied cryptography and security protocols tell us that accountability is rather difficult or expensive at best.

Looking back at stocks, such a piece of paper could not be physically divided. Nevertheless, the conventional financial theory works well with the divisibility assumption. Why? A rigorous answer might be difficult to place here but we can roughly say that

- the existence of standardized market with reliable communication network devoted to finance,

and

- the newspapers and other media which report the daily market occurrences and *physically timestamp* on them

contribute a lot. This counter-intuitive difference between paper stocks and digital setoks arise not from whether they themselves are digital or not but from their assumptions on the available infrastructures and the trustworthiness of the entities involved; Figure 1 is so important in that sense.

3 Call Option on a Simple Setok

3.1 Simple Settings

In a network life, we would want to pay for digital products in electronic cash. As reviewed later in 5.4.3, electronic cash systems could be more efficient if the monetary value of each cash or coin is less granular [17]. Some systems have only a few kinds of fixed-value coins. Therefore, if we want to allow as wide variety of electronic cash systems as possible, a fixed price would be helpful. This section assumes a setok whose price-interpretation process is an identity process[3].

We also assume here a strictly $\boldsymbol{T}$-tradable setok where $\boldsymbol{T} \neq \emptyset$. We have defined tradability only for single-valued setoks. Hence we consider a single-valued setok in this section. In the derivative theory, tradability and divisibility is important with respect to the *completeness* and *efficiency* of the market. Since a rigorous discussion would take a long time, we recommend those who are interested to consult good literatures such as [19]–[25].

We do not assume any divisibility of the setok. This is because we prefer settings less restrictive against security protocol design and implementation.

The final important decision is how to regard the setok as a "project" during the time interval we keep it. Our framework considers the contents, which suggests that the possession of a setok might yield something. Again, this section chooses the simplest story: nothing happens.

With some more specifications made, we have the following assumptions.

Assumption 3.1 *In Section 3, a* **single-valued** *setok* $(S, Y; V, H, n, 1)$ *with the following properties is studied.*

1. *The price-interpretation process is an identity process,* i.e. $Y(t) = 1$ *for all* t.
2. *The setok is* **not** *online divisible.*
3. *The setok is* **not** *offline divisible*
4. **No one can go short** *for the setok.*
5. *Each share of the setok is strictly* $\boldsymbol{T}$*-tradable.*
6. *The tradable period* $\boldsymbol{T}$ *begins at the time of purchase and is composed of a single time interval of a fixed positive length* T. *We will make it explicit by saying "*T*-tradable", where* T *is not boldfaced.*
7. *The possession of the setok has no meaning as a project and hence, in a financial term, yields no dividends.*

[3] In the conventional finance, continuous-price models were studied first, and then the biases induced by discreteness were appended [18]. In the case of the setok, we have decided to take a different approach because the discreteness would be much more significant.

8. *All the up-to-date and implicit value processes are positive and finite, i.e.* $0 < H(t) < \infty$ *and* $0 < V_j(t) < \infty$ *(j=1, 2, $\cdots$, n) for any* $t \in \mathbf{\Theta}$.

In the real world, one of the simplest derivatives is European call options written on a stock price. However, we have assumed a fixed-price setok. We are unable to write any option on the setok price. What we can do is with respect to the values.

Definition 3.1 (A European Call) *A* European call option *on the setok, purchased at time* $t = t_0$*, is defined as a derivative which provides a* right *to buy one share of the setok with a reserved explicit value* K *at a particular time* $T_m < t_0 + T$ *in the future for its fixed price, 1, regardless of the up-to-date value* $H(T_m)$ *at* $t = T_m$*. The reserved value* K *is called the* **strike value** *or the* **exercise value**, *and* T_m *is called the* **exercise date** *or the* **maturity date**, *or just simply the* **maturity**.

It should be noted that there is no obligation for the holder of the option to exercise the right on the exercise date. Obviously, he will exercise it if $H(T_m) < K$ and he won't if $H(T_m) \geq K$.

Our final setting statement is assumptions on the market.

Assumption 3.2 (Ideal Market) *We assume an ideal market which satisfies the following conditions.*

(a) *There are no transaction costs of trading both in time and in money: any transaction can be completed immediately, free of charge.*

(b) *The market is completely liquid, i.e. it is always possible to buy and/or sell unlimited quantities. In particular, it is possible to borrow unlimited amounts from the bank (by selling bonds short). The short rate* r_f *is a deterministic constant.*

(c) *There is no bid-ask spread, i.e. the selling price is equal to the buying price.*

(d) *The market is free of arbitrage.*

The four items above are common for both the setok market and the option market. In addition, the option market is assumed to have the following properties as well.

(e) *The option can be bought and sold on a market at any fraction.*

(f) *Anyone can go short for the option.*

We seem to have supposed that investors interested in derivatives are diligent enough to be connected both with the setok network and with the common financial network. Or otherwise, due to the economic benefit from options, expensive cryptographic tools are deployed to have such an ideal high-quality communication for setok-option transaction even over insecure channels. Obviously, we consider different architectures for setoks and for options. Let us have a more close look at the difference and the common features by referring to the items in Assumption 3.1 and in Assumption 3.2.

The common features, (a), (b), and (c) in Assumption 3.2, are for simplicity. The feature (a) for setoks is supported by secure timestamps; non-negligible delay may occur in the architecture of the setok world, but no one can abuse the delay for cheating. The feature (d) in Assumption 3.2 is the most common in financial theory.

With respect to setoks, no divisibility is assumed (2. and 3. in Assumption 3.1). Going short is not allowed, either (4. in Assumption 3.1). This is due to the architecture described in 2.1 at the beginning of Section 2. By contrast, with respect to options, divisibility is assumed ((e) in Assumption 3.2) and going short is allowed ((f) in Assumption 3.2). This implies that participation in the setok-option market has the same requirements as in the conventional option market: security and reliability of the resources are good enough, and participants are trusted enough.

3.2 Pricing in Discrete-Time Models

3.2.1 Single-Period Binomial Model

This subsection is the first attempt to show option pricing in the setok world. We have Assumption 3.1. To get a simple but good and instructive start, we furthermore assume that the implicit value process V is one-dimensional, *i.e.* $n = 1$, and that the value-interpretation function $h(t, v)$ is a deterministic function $h(v)$ such that $h(v) > 0$ for any $v \geq 0$. Furthermore, for a readability reason, we assign the time unity so that $T_m = 1$.

The simplest model used here is a single-period binomial model described in Fig. 2. At present ($t = 0$), the up-to-date value is $H(0) = H_0 = h(V_0)$. At the maturity, there are two possible states: $H(T_m)[\text{up}] = h(u \cdot V_0)$ and $H(T_m)[\text{down}] = h(d \cdot V_0)$ where d and u are positive constants such that $0 \leq d < 1 < u$. The former, the state after upward change, occurs with probability p_u. Hence the latter, the state after downward change, occurs with probability $1 - p_u$. You do not know these probabilities. Please find a reasonable price of the European call option. This is the problem to be solved below.

The option has a payoff of

$$C_u = \frac{\max\{0, K - h(uV_0)\}}{h(uV_0)} \tag{1}$$

in the case of the upward change. That is, if $h(uV_0) < K$, the holder of the option exercises it; he buys one share of the setok at the price 1, with the strike value K. Thanks to Definition 2.8, Assumption 3.1, and Assumption 3.2, the holder can immediately resale this share for the value-proportional price

$$S_p = \frac{K}{h(uV_0)} \cdot 1 = \frac{K}{h(uV_0)}, \tag{2}$$

and achieve a positive gain of

$$S_p - 1 = \frac{K - h(uV_0)}{h(uV_0)}. \tag{3}$$

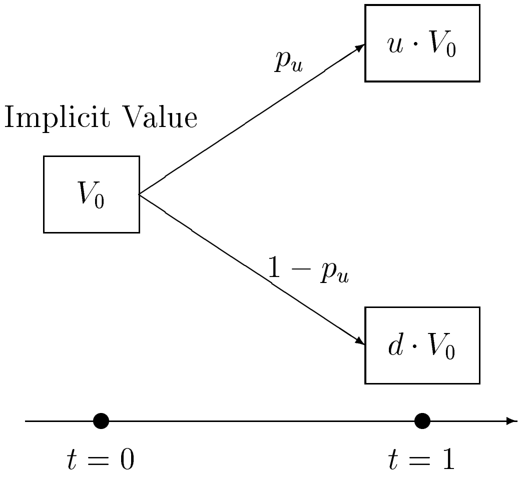

Figure 2: A single-period binomial model for pricing the European call option. The setok price is kept to be 1 all the time. At the beginning of the period ($t = 0$), the up-to-date value of the setok is $h(V_0)$. At the end of the period ($t = T_m = 1$), *i.e.* the maturity of the option, either the "upward" or the "downward" state has occurred: the former is with the option payoff C_u and the up-to-date value of the setok $h(uV_0)$ while the latter is with C_d and $h(dV_0)$, where $0 \leq d < 1 < u$. Although this illustration shows that the upward-change probability is p_u and the downward-change probability is $1 - p_u$, the pricing does not require these probabilities. They appear here just to tell you that the two states are the only possible states at $t = 1$. It is assumed that $h(uV_0) \neq h(dV_0)$, which differentiates the two states in the market as well as in the implicit world.

He is not obliged to exercise the option but he does. This is what is called the 'greedy' assumption in economics: anyone able to obtain anything of value for free will not hesitate to do so. On the contrary, if $h(uV_0) \geq K$, the holder of the option does not exercise it hence gets nothing. Eqn. (1) is a mathematical representation of this. Likewise, we find that the option has a payoff of

$$C_d = \frac{\max\{0, K - h(dV_0)\}}{h(dV_0)} \tag{4}$$

in the case of the downward change.

By using the no-arbitrage condition, it is easy to see the following lemma.

Lemma 3.1 *In the binomial single-period model described in Fig. 2, the following must hold:*

$$\frac{h(V_0)}{\max\{h(uV_0), h(dV_0)\}} \leq 1 + r_f.$$

Proof **:**

If $h(V_0)/\max\{h(uV_0), h(dV_0)\} > 1 + r_f$, then you can achieve an arbitrary large amount of gain $M\{h(V_0)/\max\{h(uV_0), h(dV_0)\} - (1 + r_f)\}$ by the following steps *with probability 1.*

1. At time $t = 0$, go short for the bank and sell the riskless T_m-bond to get M dollars.

2. Immediately after that, *i.e.* also at $t = 0$, buy M shares of the setok by using all the M dollars.

3. At time $t = T_m$, sell all the setok for the value-proportional price. This is possible because the setok is strictly T-tradable and $T > T_m$.

4. The value-proportional price is at least $h(V_0)/\max\{h(uV_0), h(dV_0)\}$. Hence what you obtain in total is at least $Mh(V_0)/\max\{h(uV_0), h(dV_0)\}$.

5. At the same time, you pay $(1 + r_f)M$ dollars for the bond.

This is not permissible. Therefore,

$$\frac{h(V_0)}{\max\{h(uV_0), h(dV_0)\}} \leq 1 + r_f.$$

Q.E.D.

Our task is to find a riskless portfolio composed of one share of setok and M European call options. Let C be the price of one share of the option (at $t = 0$). Then, our initial investment is given by

$$1 + MC. \tag{5}$$

In order to achieve risk-freeness, the portfolio must have exactly the same payoff at the maturity $t = T_m = 1$ regardless of the state (upward or downward). That is,

$$\frac{h(V_0)}{h(uV_0)} \cdot 1 + MC_u = \frac{h(V_0)}{h(dV_0)} \cdot 1 + MC_d. \tag{6}$$

Note that the first term of each side in Eqn. (6) represents the payoff resulting from one share of the setok. This is possible because the setok is strictly T-tradable and $T > T_m$.

We are afraid that it might be unclear whether the possibility means obligation or not; the holder of the setok can sell it at $t = T_m < T$ for the value-proportional price but is he *obliged* to do so? He can *wait* for a more profitable situation as far as the setok is still tradable. Why we assume that he sells the setok at $t = T_m$? A naive answer is: that is because the set of time indices is $\{0, 1\}$ in the space considered, and thus we have only today (t=0) and tomorrow (t=1). Another excuse can be found in the no-project assumption (statement 7. in Assumption 3.1). This *informally* tells us that we can have a stock-like look at the setok in terms of wealth/asset evaluation; the evaluation is based on the price for which the holder can sell it now (if he would do so). More detailed discussion in this direction would need an equilibrium theory and be beyond the scope of the first stage of our setok framework. Anyway, in the context of our current option-pricing theory, it is sufficient that we understand

- the riskless portfolio strategy is possible **if there exists** a number M which satisfies Eqn. (6) and is **allowed** in the setok/option market assumed here.

The setok values are exogenously given.

Note also that we cannot sell the setok during the time interval $t \in (0,1)$. If you were able to know the value-interpretation process time-continuously and found $H(t') < h(V_0)$ at some time $t' \in (0,1)$, then you would be tempted to sell the setok at t', before the maturity of the option. This is not what the single-period model considers. We can get no information, we can buy nothing, and we can sell nothing on the way.

After a manipulation on Eqn. (6) with the help of $h(uV_0) \neq h(dV_0)$, we have

$$M = \frac{h(V_0)}{C_d - C_u} \left\{ \frac{1}{h(uV_0)} - \frac{1}{h(dV_0)} \right\} \tag{7}$$

Because of the assumption of the ideal option market (Assumption 3.2), the portfolio is feasible regardless of the actual occurrence of M given by Eqn. (7); any $M \in \boldsymbol{R}$ is allowed.

Thus we have established a riskless portfolio. In order to achieve no arbitrage, the portfolio must have the rate of return exactly as low as the short rate r_f. Therefore, looking at the initial investment (Eqn. (5)), we notice that

$$(1 + r_f)(1 + MC) = \frac{h(V_0)}{h(uV_0)} \cdot 1 + MC_u \tag{8}$$

must hold. Let us insert Eqn. (7) into Eqn. (8). Then, after some manipulations, we obtain

$$C = \frac{pC_u + (1-p)C_d}{1 + r_f} \tag{9}$$

where p is defined by

$$p = \frac{\{(h(dV_0)\}^{-1} - (1 + r_f)\{h(V_0)\}^{-1}}{\{h(dV_0)\}^{-1} - \{h(uV_0)\}^{-1}}. \tag{10}$$

The story above can be summarized as the following theorem.

Theorem 3.1 (Option-Pricing Formula (Single-Period Model)) *In the binomial single-period model described in Fig. 2, let us consider a European call option defined by Definition 3.1 under Assumption 3.1 and Assumption 3.2. Choose the option's maturity T_m as a time unit and assume that the short rate of interest is a constant r_f for the time unit. Let the price process and the strike value of the option be $C(t)$ and K, respectively. Then, the following pricing formula holds.*

$$C(0) = \frac{pC_u + (1-p)C_d}{1 + r_f}$$

where

$$C_u = \frac{\max\{0, K - h(uV_0)\}}{h(uV_0)}$$

$$C_d = \frac{\max\{0, K - h(dV_0)\}}{h(dV_0)}$$

$$p = \frac{\{(h(dV_0)\}^{-1} - (1 + r_f)\{h(V_0)\}^{-1}}{\{h(dV_0)\}^{-1} - \{h(uV_0)\}^{-1}}.$$

We are happy because the pricing does not need p_u. This feature can be interpreted by the following statements:

- Pricing Theorem 3.1 does not need the objective measure. Instead, it looks simple and sound with the *risk-neutral* measure,

which coincides with the well-known feature of the basic financial option pricing theories. This will be soon revisited in 3.2.2.

We are also happy to see that

- no divisibility assumption on the setok is needed,

and that

- the setok is allowed to have a finite lifetime in tradability.

Both go well with the basic architecture described in Fig. 1. From the engineering point of view, such a less restrictive situation most likely allows cheaper and more efficient protocols which are suitable for general customers.

3.2.2 Hedging Probability and Martingale Measure

Before proceeding, let us further investigate the meaning of p in the pricing formula (Theorem 3.1).

Lemma 3.2 (Hedging Probability) *If $h(V_0)/\min\{h(uV_0), h(dV_0)\} \geq 1 + r_f$, the parameter p given in Theorem 3.1 satisfies $0 \leq p \leq 1$. In this case, we refer to p as the hedging probability.*

Proof **:**

We have assumed that $h(v) > 0$ for any $v \geq 0$ and that $h(uV_0) \neq h(dV_0)$.

When $h(uV_0) > h(dV_0)$, we have $h(V_0)/h(dV_0) \geq 1 + r_f$ because of the assumption $h(V_0)/\min\{h(uV_0), h(dV_0)\} \geq 1 + r_f$. $h(uV_0) > h(dV_0)$ of course implies $1/h(dV_0) > 1/h(uV_0)$. Consequently,

$$p = \frac{\{(h(dV_0)\}^{-1} - (1 + r_f)\{h(V_0)\}^{-1}}{\{h(dV_0)\}^{-1} - \{h(uV_0)\}^{-1}} = \frac{\frac{h(V_0)}{h(dV_0)} - (1 + r_f)}{h(V_0)\left\{\frac{1}{h(dV_0)} - \frac{1}{h(uV_0)}\right\}} \geq 0.$$

By using $h(uV_0) > h(dV_0)$ and Lemma 3.1, we have $h(V_0)/h(uV_0) \leq 1 + r_f$. We remember $1/h(dV_0) > 1/h(uV_0)$. Hence

$$1 - p = \frac{(1 + r_f)\{h(V_0)\}^{-1} - \{(h(uV_0)\}^{-1}}{\{h(dV_0)\}^{-1} - \{h(uV_0)\}^{-1}} = \frac{(1 + r_f) - \frac{h(V_0)}{h(uV_0)}}{h(V_0)\left\{\frac{1}{h(dV_0)} - \frac{1}{h(uV_0)}\right\}} \geq 0.$$

When $h(uV_0) < h(dV_0)$, we have $h(V_0)/h(uV_0) \geq 1 + r_f$ because of the assumption $h(V_0)/\min\{h(uV_0), h(dV_0)\} \geq 1 + r_f$. $h(uV_0) < h(dV_0)$ of course implies $1/h(dV_0) < 1/h(uV_0)$. Consequently,

$$1 - p = \frac{(1 + r_f) - \frac{h(V_0)}{h(uV_0)}}{h(V_0)\left\{\frac{1}{h(dV_0)} - \frac{1}{h(uV_0)}\right\}} \geq 0.$$

By using $h(uV_0) < h(dV_0)$ and Lemma 3.1, we have $h(V_0)/h(dV_0) \leq 1 + r_f$. We remember $1/h(dV_0) < 1/h(uV_0)$. Hence

$$p = \frac{\frac{h(V_0)}{h(dV_0)} - (1 + r_f)}{h(V_0)\left\{\frac{1}{h(dV_0)} - \frac{1}{h(uV_0)}\right\}} \geq 0.$$

Q.E.D.

Proposition 3.1 (A Martingale Measure) *Let us* **discount** *the option price process $C(t)$ by the (***riskless***) short rate r_f, and define a process $\bar{C}(t)$ by*

$$\begin{aligned} \bar{C}(0) &= C(0) \\ \bar{C}(1) &= (1 + r_f)^{-1} C(1). \end{aligned}$$

Then,

1. *The hedging probability p provides a probability measure if we* **assign** *p as the probability of the upward change and $1 - p$ as the downward one.*

2. *Under this measure, the discounted price process $\bar{C}(t)$ has the martingale property such that*

$$\bar{C}(0) = E_0\left[\bar{C}(1)\right]$$

where E_0 denotes the expectation operator conditioned by the available information at $t = 0$.

Proof **:**

Let us denote the state after the upward change by "up", and that by the downward change by "down".

The first statement is trivial from the definition given by Eqn. (10) and Lemma 3.2.

To prove the second statement, please note that the no-arbitrage requirement gives $C(1)[\text{up}] = C_u$ and $C(1)[\text{down}] = C_d$; *i.e.* the option price at the maturity must be equal to the payoff. Therefore, we have

$$\begin{aligned} E_0\left[\bar{C}(1)\right] &= p\bar{C}(1)[\text{up}] + (1 - p)\bar{C}(1)[\text{down}] \\ &= p(1 + r_f)^{-1}C(1)[\text{up}] + (1 - p)(1 + r_f)^{-1}C(1)[\text{down}] \\ &= (1 + r_f)^{-1}\{pC_u + (1 - p)C_d\} \end{aligned}$$

Theorem 3.1 says that this equals to $C(0)$, which is by definition equal to $\bar{C}(0)$. ***Q.E.D.***

3.2.3 Multiple-Period Binomial Model

By repeating the binomial process, we can easily extend the single-period model to a multiple-period model (Fig. 3). Let the maturity T_m be 1 as in the previous subsection and divide the time interval $[0, 1]$ into a large number of periods, say, N periods: $[0, 1/N)$, $[1/N, 2/N)$, $\cdots$, $[(N-1)/N, 1)$. We must pay attention to three things:
(i) The short rate is defined as a rate of interest for a time unit. Hence we use r_f/N for each period.

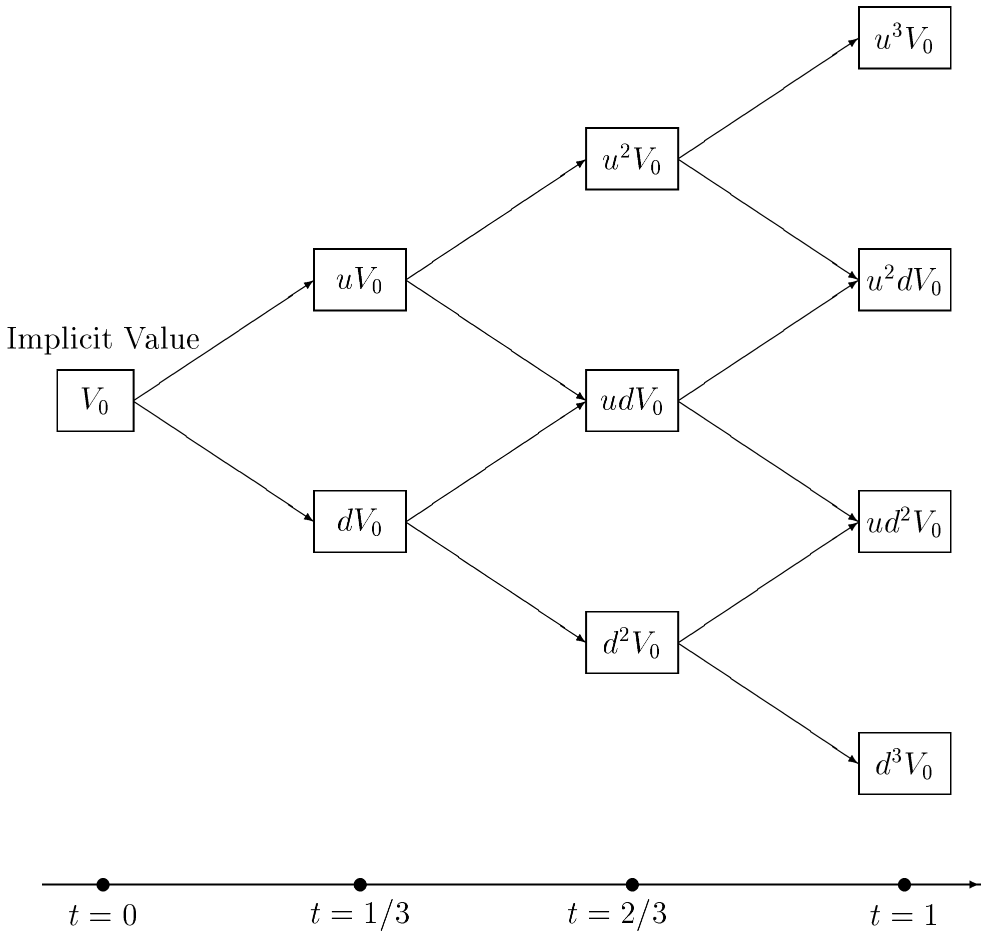

Figure 3: A multiple-period binomial model for pricing the European call option. For drawing convenience, the illustration has only $N = 3$ periods. The setok price is kept to be 1 all the time. At the beginning of the period ($t = 0$), the up-to-date value of the setok is $h(V_0)$. At the end of the period ($t = T_m = 1$), *i.e.* the maturity of the option, we have N possible states denoted by the number j of upward changes which have occurred. We also denote each state at time $t = i/N$ by the number j of upward changes which have occurred. We suppress the transition probability, which was denoted by p_u and $1-p_u$ in the case of the single-period model, because they are not used in the pricing. We assume that $H(i/N)[j] \neq H(i/N)[k]$ $(j \neq k)$ for any $i \in \{1, 2, \cdots, N\}$.

(ii) At each edge of the periods, *i.e.* $t = i/N$ $(i = 1, 2, \cdots, N)$, the state is determined by how many upward changes have occurred. Let j be the number of upward changes which have occurred during the first i periods. Then the up-to-date value of the setok at $t = i/N$ is given by

$$h\left(u^j d^{i-j} V_0\right). \tag{11}$$

In particular, the payoff of the option, which must be equal to the option price at the maturity, is given by

$$C(1)[j] = \frac{\max\{0, K - h(u^j d^{N-j} V_0)\}}{h(u^j d^{N-j} V_0)}. \tag{12}$$

(iii) In general, the hedging probability p depends on the state at the beginning of the period. For the period $[i/N, (i+1)/N)$,

$$\begin{aligned} p &= p\left(\frac{i}{N}\right)[j] \\ &= \frac{\{h(d \cdot u^j d^{i-j} V_0)\}^{-1} - \left(1 + \frac{r_f}{N}\right)\{h(u^j d^{i-j} V_0)\}^{-1}}{\{h(d \cdot u^j d^{i-j} V_0)\}^{-1} - \{h(u \cdot u^j d^{i-j} V_0)\}^{-1}} \\ &= \frac{\{h(u^j d^{i-j+1} V_0)\}^{-1} - \left(1 + \frac{r_f}{N}\right)\{h(u^j d^{i-j} V_0)\}^{-1}}{\{h(u^j d^{i-j+1} V_0)\}^{-1} - \{h(u^{j+1} d^{i-j} V_0)\}^{-1}} \end{aligned} \tag{13}$$

if j upward changes have occurred during the first i periods. Thus p is an adapted process.

Due to the property (iii), it is in general cumbersome to explicitly write the pricing formula. Instead, we had better firstly show the *backward algorithm* for computation:
Algorithm 1:

1. Stand at $t = (N-1)/N$ and compute $C\left(\frac{N-1}{N}\right)[j]$ $(j = 0, 1, \cdots, N-1)$ by using (or carefully speaking, "interpreting") Theorem 3.1 with the cares (i), (ii), and (iii) listed above. Thus you have

$$C\left(\frac{N-1}{N}\right)[j] = \frac{p\left(\frac{N-1}{N}\right)[j]C(1)[j+1] + \{1 - p\left(\frac{N-1}{N}\right)[j]\}C(1)[j]}{1 + \frac{r_f}{N}}$$

   for $j = 0, 1, \cdots, N-1$, where $C(1)[j]$ $(j = 0, 1, \cdots, N)$ and $p\left(\frac{N-1}{N}\right)[j]$ $(j = 0, 1, \cdots, N-1)$ are given by Eqn. (12) and Eqn. (13), respectively.

2. Go back to $t = (N-2)/N$ and note that $C\left(\frac{N-1}{N}\right)[j]$ represents what you obtain if you sell one share of option at the state j at $t = (N-1)/N$. Compute $C\left(\frac{N-2}{N}\right)[j]$ $(j = 0, 1, \cdots, N-1)$ by using (or carefully speaking, "interpreting") Theorem 3.1. In place of the payoffs, use $C\left(\frac{N-1}{N}\right)[j]$. Thus you have

$$C\left(\frac{N-2}{N}\right)[j] = \frac{p\left(\frac{N-2}{N}\right)[j]C\left(\frac{N-1}{N}\right)[j+1] + \left\{1 - p\left(\frac{N-2}{N}\right)[j]\right\}C\left(\frac{N-1}{N}\right)[j]}{1 + \frac{r_f}{N}}$$

   where $C\left(\frac{N-1}{N}\right)[j]$ $(j = 0, 1, \cdots, N-1)$ are given by the previous step. $p\left(\frac{N-2}{N}\right)[j]$ $(j = 0, 1, \cdots, N-2)$ are given by Eqn. (13).

3. Repeat the above procedure until you reach $t = 0$ and obtain

$$C(0) = \frac{p(0)[0]C(1/N)[1] + \{1 - p(0)[0]\}C(1/N)[0]}{1 + \frac{r_f}{N}}.$$

Next, let us explore a situation which gives an easy-to-write formula. Our concern is the dependence of the hedging probability on the up-to-date value of the setok at the beginning of each period. We want to avoid this dependence by assigning a specific form of value-interpretation function h.

Let us consider

$$h(v) = av^b \tag{14}$$

where a and b are positive constants. Then, at each period and each state, we can use the same hedging probability given by

$$p = \frac{d^{-b} - \left(1 + \frac{r_f}{N}\right)}{d^{-b} - u^{-b}}. \tag{15}$$

By using Algorithm 1, we have

$$C(1)[j] = \frac{\max\{0, K - a(u^j d^{N-j} V_0)^b\}}{a(u^j d^{N-j} V_0)^b}, \tag{16}$$

$$C\left(\frac{N-1}{N}\right)[j] = \frac{pC(1)[j+1] + (1-p)C(1)[j]}{1 + \frac{r_f}{N}}, \tag{17}$$

$$\begin{aligned} C\left(\frac{N-2}{N}\right)[j] &= \left(1 + \frac{r_f}{N}\right)^{-1} \left\{pC\left(\frac{N-1}{N}\right)[j+1] + (1-p)C\left(\frac{N-1}{N}\right)[j]\right\} \\ &= \left(1 + \frac{r_f}{N}\right)^{-2} \left\{p^2 C(1)[j+2] + 2p(1-p)C(1)[j+1] + (1-p)^2 C(1)[j]\right\}, \end{aligned} \tag{18}$$

$\cdots$, and finally

$$\begin{aligned} C(0) &= \left(1 + \frac{r_f}{N}\right)^{-N} \sum_{j=0}^{N} \binom{N}{j} p^j (1-p)^{N-j} C(1)[j] \\ &= \left(1 + \frac{r_f}{N}\right)^{-N} \sum_{j=0}^{N} \binom{N}{j} p^j (1-p)^{N-j} \frac{\max\{0, K - a(u^j d^{N-j} V_0)^b\}}{a(u^j d^{N-j} V_0)^b}. \end{aligned} \tag{19}$$

Eqn. (19) can be easily proved by mathematical induction outlined above. Intuitively, the following statements would be helpful.

- There are $\binom{N}{j}$ paths between the start ($t = 0$) and each final state j at the maturity ($t = 1$).
- Every path must experience exactly N changes.
- Each upward change makes the payoff be multiplied by $p\left(1 + \frac{r_f}{N}\right)^{-1}$.

- Each downward change makes the payoff be multiplied by $(1-p)\left(1+\frac{r_f}{N}\right)^{-1}$.
- So the contribution of each path to the state j with the payoff $C(1)[j]$ is

$$\left(1+\frac{r_f}{N}\right)^{-N} p^j(1-p)^{N-j}C(1)[j]$$

Thus, although it seems an artificial example, we have obtained a simple closed-form pricing formula. We would like to summarize it.

Theorem 3.2 (Option-Pricing Formula (Multiple-Period Model)) *In the binomial multiple-period model described in Fig. 3, let us consider a European call option defined by Definition 3.1 written on a setok which has the value-interpretation function $h(v) = av^b$ (a, b : positive constants). We have Assumption 3.1 and Assumption 3.2 as well as the following two assumptions:*

1. *The short rate of interest is a constant $\frac{r_f}{N}$ during each period of length $1/N$.*
2. *The maturity is $T_m = 1$ (chosen as the time unit).*

Let the price of the option now ($t = 0$) and the strike value of the option be $C(0)$ and K, respectively. Then, the following pricing formula *holds.*

$$C(0) = \left(1+\frac{r_f}{N}\right)^{-N}\sum_{j=0}^{N}\binom{N}{j}p^j(1-p)^{N-j}\frac{\max\{0, K-a(u^jd^{N-j}V_0)^b\}}{a(u^jd^{N-j}V_0)^b}$$

where

$$p = \frac{d^{-b}-\left(1+\frac{r_f}{N}\right)}{d^{-b}-u^{-b}}.$$

If we further assume $K > aV_0^bd^N$, which is the condition for the option to have non-zero probability for a positive payoff at the maturity, then the formula can be expressed in a more (economically) instructive way:

$$C(0) = \left(1+\frac{r_f}{N}\right)^{-N}K\sum_{j=0}^{n'}\binom{N}{j}\frac{p^j(1-p)^{N-j}}{a(u^jd^{N-j}V_0)^b} - \left(1+\frac{r_f}{N}\right)^{-N}\sum_{j=0}^{n'}\binom{N}{j}p^j(1-p)^{N-j}$$

where

$$n' = \left[\frac{\ln\left(\frac{K}{aV_0^bd^N}\right)}{b\ln\left(\frac{u}{d}\right)}\right].$$

Although Theorem 3.2 mentions merely about the option price at $t = 0$, Algorithm 1 gives us whole the price process at $t \in [0, 1/N, 2/N, \cdots, 1]$. It should be also noted that the multiple-period pricing formula, Eqn. (19), holds even if the transition probabilities (p_u for the upward change and $1-p_u$ for the downward change) change period by period as far as both the probabilities are positive. Suppose that you are a great person: security minister of a large country. You are happy if the setok market is stable in terms of the up-to-date values. The value-interpretation function is fixed as the form of Eqn. (14). You have made best political effort to achieve better stability. Your effort may contribute to

1. the reduction of the **volatility** factors of the value-interpretation function, *i.e.* a and b,
2. the reduction of the volatility factor of the implicit value process, *i.e.* $|u-d|$, or
3. the adaptive control of the transition probability; for instance, $p_u > 1 - p_u$ when $H(t)$ is lower than a certain desirable value H_0 and $p_u < 1 - p_u$ when $H(t) > H_0$.

The first two may be detected and you could be proud of it if you watch the setok and the option price processes, whereas the last one cannot. **There can be an administrative strategy which stabilizes the underlying setok with no influence on the option price.**

Before ending this subsection, we would like to place again the question on the trade of the setok. This was discussed in the single-period model: "The holder of the setok can *wait* for a more profitable situation as far as the setok is still tradable. Why we assume that he sells the setok at $t = T_m$?" In the case of Algorithm 1 for deriving the pricing formula in the multiple-period model, the evaluation regarding the final period may be easy to accept after the discussion in the single-period model. So the remaining questions would be:

- The holder of the setok can *wait* for a more profitable situation as far as the setok is still tradable (and in fact, it is tradable under the assumption $T_m < T$). Why we assume that he sells the setok at each $t = i/N$ $(i = 1, 2, \cdots, N-1)$ and *reshape* his portfolio period by period?
- Is each period long enough for the investors to operate such a dynamic portfolio strategy?

Regarding the first question, we may have the same discussion as in the single-period model as far as we look at each state of each period as if it were the beginning of the single-period model. Detailed discussion in total may lead us to equilibrium theory, which is out of scope of this paper. The important thing is the fact that each of the dynamically constructed portfolios

- is feasible and
- satisfies the riskless property and the no-arbitrage condition.

Regarding the second question, recall the ideal market assumption (Assumption 3.2), in particular the statement (a). There is no transaction costs both in time and in money. From the engineering point of view, this would be very demanding. But we have assumed it. From the users' point of view, there are two excuses. One is the "diligent investor" statement which have followed Assumption 3.2. The other is a setok-specific scenario:

users of the content tend to dislike both (i) an old information and (ii) huge and possibly expensive storage of setoks. For example, once an entity has verified a digital signature, he deletes the certificate used[4].

3.3 Pricing in a Continuous-Time Model

3.3.1 Model Description

The previous subsection 3.2 has investigated the models which are discrete both in time and in values. What happens if we consider not discrete but somewhat continuous models? Specifically, we want to model a situation in which

- we can have trades whenever we wish,
- we can always observe the market, and
- the implicit values can take any non-negative real values.

We consider the following model.

Assumption 3.3 (Continuous-Time Model) *In Section 3, we are investigating setok* $(S, Y; V, H, n, 1)$ *under Assumption 3.1, and the European call option on it. Let* $C(t) = c(t, H(t))$ *be the price process of the option.*

As a simple continuous-time model, we further assume the followings.

- *The function* $c(t, h)$ *is a* $C^{1,2}$*-mapping.*
- *The dynamics of the (observable) up-to-date value process* H *is given by*

$$dH = \mu(t, H(t))Hdt + \sigma(t, H(t))HdW$$

  where $\mu(t, H(t))$ *and* $\sigma(t, H(t))$ *are adapted processes and* W *is a Wiener process under the objective measure.*
- *Define* $G(t) = \{H(t)\}^{-1}$ *and corresponding occurrence as* $g = 1/h$*. We sometimes regard* c *as a function of* t *and* g*. To avoid confusion, we write* $\hat{c}(t, g) = c(t, 1/g)$*, where we assume the function* $\hat{c}$ *is also a* $C^{1,2}$*-mapping.*
- *The price process of the riskless asset is described by the dynamics*

$$dB(t) = r_f B(t)dt$$

  where the short rate r_f *is a deterministic constant.*

[4] This is a story of light-weight security. Digital forensics may require more for future dispute settlements [26], [27]. Technologies available for such purposes — secure audit log — are discussed in [28]–[30], for instance.

In general, the process H driven by the assumed dynamics

$$dH = \mu H dt + \sigma H dW \tag{20}$$

in Assumption 3.3 is said to be the *geometric Brownian motion with drift* if μ and σ are deterministic constants. In this case, the absolute change in H over any finite time interval is *log-normally* distributed. The geometric Brownian motion with drift appear in a lot of random variables in the real society. We estimate μ and σ by using the observed market data; they are exogenously given parameters.

In fact, Assumption 3.3 is mathematically quite similar to the well-known Black-Scholes model[31] for pricing options on stocks. However, it is worth noting that Assumption 3.1 says the setok is neither online nor offline divisible. In addition, we cannot go short for it. These properties are different from those of stocks.

3.3.2 Pricing

We wish to derive a pricing formula for the European call option purchased at $t = 0$ and matured $t = T_m$, where T_m is not necessarily equal to 1 but smaller than T. Firstly, let us define an adapted process $G(t)$ by

$$G(t) = g(t, H(t)), \tag{21}$$

where

$$g(t, h) = \frac{1}{h}. \tag{22}$$

By using Itô's Lemma and Eqn. (22), the dynamics of this process is given by

$$\begin{aligned} dG &= \left\{ g_t + \mu H g_h + \frac{1}{2}\sigma^2 H^2 g_h h \right\} dt + \sigma H g_h dW \\ &= \left\{ 0 - \frac{\mu H}{H^2} + \frac{1}{2}\sigma^2 H^2 \frac{2}{H^3} \right\} dt - \frac{\sigma H}{H^2} dW \\ &= \left(-\frac{\mu}{H} + \frac{\sigma^2}{H} \right) dt - \frac{\sigma}{H} dW \end{aligned} \tag{23}$$

where we denote partial derivatives by subscripts:

$$\frac{\partial g}{\partial t} = g_t, \ \frac{\partial g}{\partial h} = g_h, \ \frac{\partial^2 g}{\partial h^2} = g_{hh}. \tag{24}$$

In the rest of this paper, we may use this type of notation without clearly stating it as far as the context is clear.

Secondly, let us consider a portfolio composed of one setok and M options. The portfolio is dynamically changed, over and over again. As in the discrete-time multiple-period model, let us think of any infinitesimal time interval of length dt. Each dynamics is given in the form of SDE. Let F be the monetary value (in terms of the initial investment at the beginning of the infinitesimal time interval) of this portfolio:

$$F = 1 + MC. \tag{25}$$

We sell the setok for the value-proportional price and immediately buy one setok with the up-to-date value for the fixed up-to-date price 1 at the end of the time interval. By assumption, these procedures take no time and are allowed even in the case of the infinitesimal time interval. Thus, over the time interval, the "resale and buy" brings

$$\frac{G+dG}{G}-1=\frac{dG}{G} \tag{26}$$

and tells us that the dynamics of F is given by

$$dF=\frac{dG}{G}+MdC \tag{27}$$

We have to be careful about the fact that **stochastic differentials are the expected value at the beginning of the time interval.** So a more instructive notation for Eqn. (27) would be

$$E_t[dF]=\frac{E_t[dG]}{G(t)}+M(t)E_t[dC], \tag{28}$$

where E_t denotes the expectation operator conditioned by the information available at time t. We apply Itô's Lemma for dC, and insert it as well as Eqn. (23) into Eqn. (27). Then we obtain[5]

$$\begin{aligned} dF &= \left\{M\left(c_t+\mu H c_h+\frac{\sigma^2}{2}H^2 c_{hh}\right)-\mu+\sigma^2\right\}dt+\left(M\sigma H c_h-\sigma\right)dW \\ &= \left\{M\left(\hat{c}_t-\mu G\hat{c}_g+\sigma^2 G\hat{c}_g+\frac{\sigma^2}{2}G^2\hat{c}_{gg}\right)-\mu+\sigma^2\right\}dt-\sigma\left(MG\hat{c}_g+1\right)dW. \end{aligned} \tag{29}$$

Thanks to the divisibility of the option, by choosing

$$M=-\frac{1}{G\hat{c}_g}, \tag{30}$$

we can make the portfolio risk-free, *i.e.* force the diffusion dW-term to be zero. Note that M can change over time. This is a dynamic replication of the risk-free asset.

Since any risk-free asset must have r_f as the rate of return, we have

$$M\left(\hat{c}_t-\mu G\hat{c}_g+\sigma^2 G\hat{c}_g+\frac{\sigma^2}{2}G^2\hat{c}_{gg}\right)-\mu+\sigma^2=r_f F. \tag{31}$$

It should be noted that $F=F(t)$ on the right-hand side of Eqn. (31).

Finally, we insert Eqn. (25) and Eqn. (30) into Eqn. (31). The resultant relation must hold for any occurrence of the adapted process G. So let us use g instead of G to obtain the *partial differential equation (PDE)*

$$\frac{\sigma^2}{2}g^2\hat{c}_{gg}+r_f(g\hat{c}_g-\hat{c})+\hat{c}_t=0. \tag{32}$$

We solve this PDE under the boundary condition

$$\hat{c}(T_m,g)=\max\{0,Kg-1\}, \tag{33}$$

[5] It is elementary to see that $c_h=-G^2\hat{c}_g$ and $c_{hh}=2G^3\hat{c}_g+G^4\hat{c}_{gg}$.

which says that the option price at the maturity must be equal to the payoff at that time[6]. The following theorem gives the summary and the notational remark.

Theorem 3.3 (Boundary Value Problem for Option Pricing) *Consider the European call option defined by Definition 3.1 written on the setok under Assumption 3.3. The maturity of the option is T_m and the strike value is K. $H(t)$ is the up-to-date value process of the setok.*

Then the only pricing function of the form $C(t) = c(t, H(t))$ consistent with the no-arbitrage condition is obtained when $c(t,h) = \hat{c}(t, 1/h)$ and $\hat{c}(t,g)$ is the solution of the boundary value problem

$$\frac{\sigma^2}{2} g^2 \hat{c}_{gg} + r_f(g\hat{c}_g - \hat{c}) + \hat{c}_t = 0$$

$$\hat{c}(T_m, g) = \max\{0, Kg - 1\}$$

in the domain $[0, T_m] \times \boldsymbol{R}_+$.

In general, it is difficult to obtain an analytical closed-form solution for the boundary value problem in Theorem 3.3. However, we do not have to be disappointed. We can use numerical approach to obtain approximate solutions. The form of the PDE considered is not really strange.

We have to mention an extremely simple case: if μ and σ are deterministic constants, a closed-form solution is easily obtained as follows.

Theorem 3.4 (Option-Pricing Formula (Continuous-Time Model)) *Let the up-to-date value process follow the geometric Brownian motion with drift, i.e. μ and σ be deterministic constants. Then Theorem 3.3 yields the pricing formula $C(t) = c(t, H(t))$, where*

$$c(t,h) = \frac{K}{h} N\left[d_1(t,h)\right] - \exp\left\{-r_f(T_m - t)\right\} N\left[d_2(t,h)\right]$$

where N is the cumulative distribution function for the standard normal distribution, i.e.

$$N[d] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{d} \exp\left(-\frac{x^2}{2}\right) dx$$

and

$$d_1(t,h) = \frac{1}{\sigma\sqrt{T_m - t}} \left\{ \ln\left(\frac{K}{h}\right) + \left(r_f + \frac{\sigma^2}{2}\right)(T_m - t) \right\},$$

$$d_2(t,h) = d_1(t,h) - \sigma\sqrt{T_m - t}.$$

[6] This must hold for any state at the maturity.

Let us see on which parameters the option price in Theorem 3.4 depends. It depends on the diffusion σ, the maturity date T_m, the short rate r_f, the up-to-date value h, and of course the strike value K. By contrast, it does not depend on the drift μ and the length of the tradability period T.

Remark 3.1

- *In the continuous-time model, the maturity T_m is not necessarily equal to the time unit.*
- *Theorem 3.3 holds even if μ and σ are time-variant and stochastic as far as they are adapted processes.*
- *Typically, numerical analysis can be used to solve the boundary value problem.*
- *The PDE (Eqn. (32)) holds as long as we consider a European-type option and the pricing function is of the form $C(t) = c(t, H(t))$ consistent with the no-arbitrage, regardless of the payoff at the maturity. Therefore, in the case of another European-type option, all we have to do is to replace the boundary condition (Eqn. (33)) with an appropriate condition which describes the payoff.*

3.3.3 Analysis of the Option-Pricing Formula

In order to investigate the characteristics of the option-pricing formula, we plot the option prices given by Theorem 3.4 with changing the up-to-date value $H(0) \in [80, 120]$. Because the price at $t > 0$ equals to the current ($t = 0$) price of an option with maturity $T_m - t$, we analyze $C(0)$ only and denote it by C in the following. We choose one year as the time unit. We interpret the short rate r_f into the intuitive (yearly) rate r of interest for the bank account by

$$r = \exp(r_f) - 1 \tag{34}$$

and we use percentage representation when we refer to r.

The basic parameter assignments are as follows.

Maturity: $T_m = 1$ [year]

Volatility: $\sigma = 0.2$

Exercise Value: $K = 100$

Short Rate: $r = 0.5$ [%]

We are going to show four figures. Since smaller up-to-date values mean the option holders are in better positions now, the curves are monotone decreasing in each figure.

Firstly, we investigate the effect of the maturity. The plots for $T_m = 0.5$, 1, and 2 are given in Fig. 4. If the maturity is further away from now, things become more uncertain. **The uncertainty relaxes both chance and risk;** curves for larger T_m are less changing. Roughly speaking, larger T_m bring lower option prices for $H(0) < K = 100$;

the currently better position of the option holder is less evident under larger uncertainty. Also roughly speaking, larger T_m bring higher option prices for $H(0) > K = 100$; the currently worse position of the option holder is also less evident under larger uncertainty.

Secondly, we investigate the effect of the volatility σ. The plots for $\sigma = 0.1$, 0.2, and 0.4 are given in Fig. 5. If the volatility is larger, things would become more uncertain. Therefore, the effect is quite similar to that of the maturity; the uncertainty relaxes both chance and risk, and curves for larger σ are less changing.

Thirdly, we investigate the effect of the exercise value K. The plots for $K = 80$, 100, and 120 are given in Fig. 6. It is obvious that larger exercise values mean currently better positions of the option holder. Figure 6 represents this feature; larger exercise values bring higher option prices. It should be noted that the option price almost equals to the fixed setok price, *i.e.* $C \simeq 1 = Y(t)$, when the current position of the holder is neutral (*i.e.* when $H(0) \simeq K$).

Finally, we investigate the effect of the short rate. The plots for $r = 0.01$, 0.5, 1.0, and 10.0 [%] are given in Fig. 7. In general, higher short rates make investments more profitable. Figure 7 represents this feature; larger short rates bring higher option prices. However, realistic short rates show little difference. Only the unrealistically high rate ($r = 10.0\%$) dominates evidently.

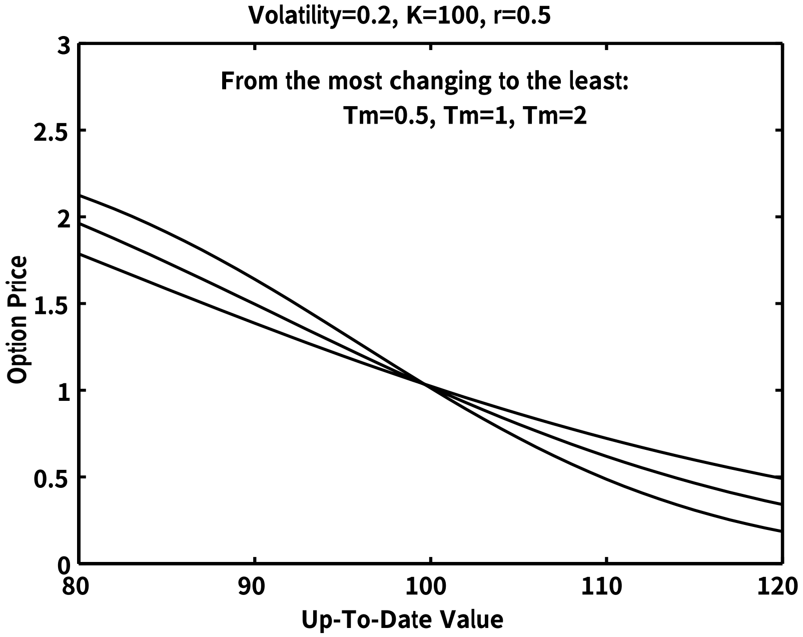

Figure 4: European call option price against up-to-date values of the setok whose price is fixed to be 1. The curves for the maturities $T_m = 0.5$, 1, and 2 are shown. Further maturities bring less changing curves by relaxing chances (for smaller up-to-date values) and risks (for larger up-to-date values).

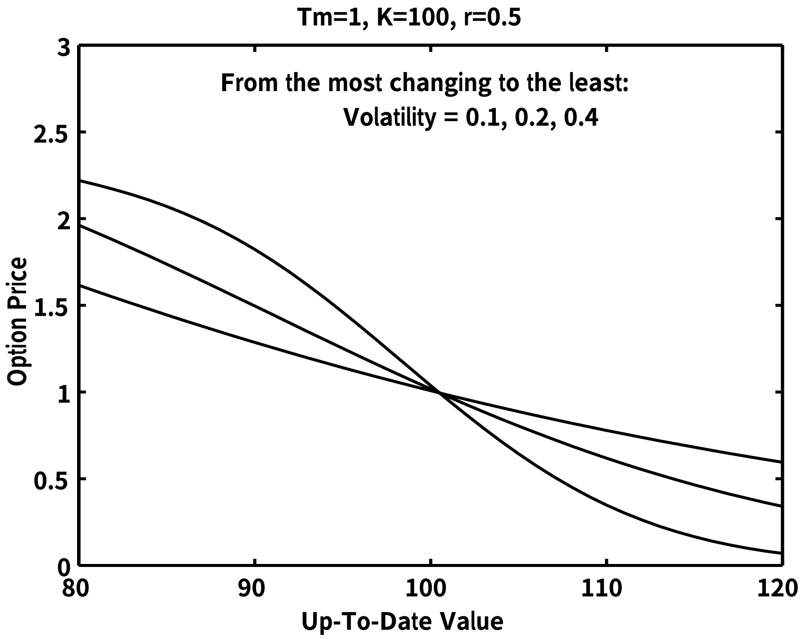

Figure 5: European call option price against up-to-date values of the setok whose price is fixed to be 1. The curves for the volatilities $\sigma = 0.1$, 0.2, and 0.4 are shown. Larger volatilities bring less changing curves by relaxing chances (for smaller up-to-date values) and risks (for larger up-to-date values).

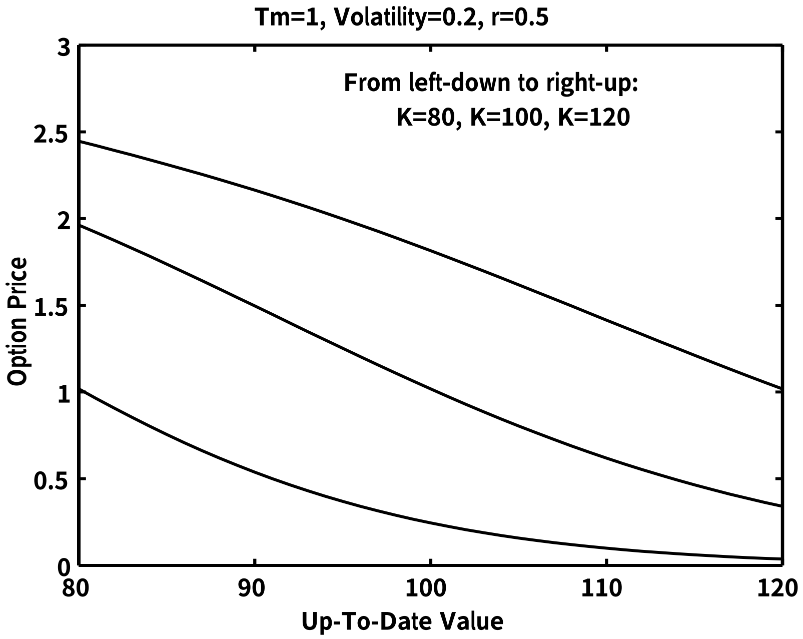

Figure 6: European call option price against up-to-date values of the setok whose price is fixed to be 1. The curves for the exercise values $K = 80$, 100, and 120 are shown. Higher exercise values mean currently better positions of the option holders, and hence bring higher option prices.

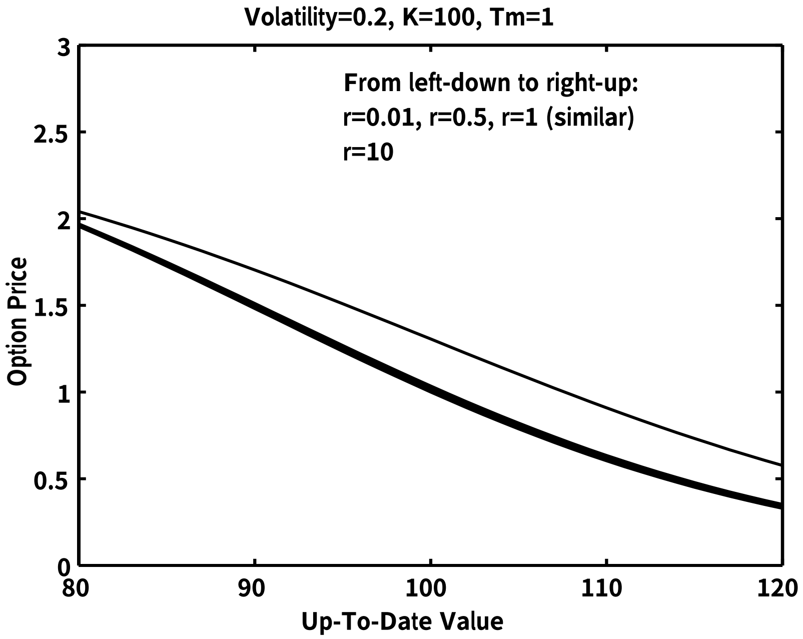

Figure 7: European call option price against up-to-date values of the setok whose price is fixed to be 1. The curves for the (yearly) short rates of interest $r = 0.01$, 0.5, 1.0 and 10.0 [%] are shown. Higher short rates make investments more profitable and give higher option prices.

4 Compromise and Revocation

4.1 Observation and Implication

Suppose again that you are a great person: security minister. The setok world of your concern works mostly well but there are possibility of revocation: implicit values can be compromised (*i.e.* discontinuously reduced to be zero), and the compromise can cause a sudden and significant ruin of the corresponding up-to-date values and/or price. Depending on the contents, this ruin can be viewed as a revocation. For example, a certificate with zero confidence would be no longer valid as itself, and no longer tradable. You want to watch how often such a disaster *is likely to* happen. What can you do for that?

Of course, you can watch the market because your position is so important that you have resources at least as good as the object providers' and servers'. You can analyse the statistics. If the revocation frequency so far is not really high, you are probably happy. But you may still concern about the setoks which have never experienced revocation but may face it sometime in the future. You want to know the public opinion or public fear. You may distribute a questionnaire which places a question: "How often do you think the setok $(S, Y; V, H, n, m)$ is likely to have revocation in value? Please specify it in percentage." This may cost a lot and the result may be too subjective. It takes time, too. The purpose of this section is to make an attempt to obtain less subjective opinion by observing the setok/option market: we expect that some parameters related with the compromise are *implied* by the market data including the option price. Thus we wish to have an option-pricing theory under a risk of compromise.

4.2 Extended Settings

In this section, we study again a continuous-time model. As for the underlying setok, we mostly follow Assumption 3.1. The fundamental difference is the possibility of compromise and the response to it; the setok considered is compromise-responsive in value. Furthermore, we suppose that the primary meaning of compromise is a significant damage on the effectiveness of the setok itself. Thus we change the assumptions on tradability and project value:

(Non-Strict Tradability) The tradability is assumed to be **not** strict here. Although the setok is T-tradable, T is **stochastic**. Let $H(0) > 0$ and $T(0) = T_0 > 0$. As long as the up-to-date value $H(t)$ is positive, T keeps the initial value T_0. However, in the case of revocation, the tradability is ruined; $T(t) = 0$ for any t such that $H(t) = 0$. But the holders of the setok do not have to be completely discouraged. In place of the tradability, a refundability arises.

(Project Opportunity) As long as the up-to-date value $H(t)$ is larger than a threshold value H_θ, each share of the setok gives the holder an opportunity of dividend proportional to the length of time interval. We model this as a Poisson process. The "no project" assumption which has been used so far in this paper is a special case such that the intensity of the Poisson process is zero.

We specify this situation formally.

Assumption 4.1 (Setok with Revocation) *In Section 4, a* single-valued *setok* $(S, Y; V, H, n, 1)$ *with the following properties is studied.*

1. *The price-interpretation process is an identity process,* i.e. $Y(t) = 1$ *for all* t.

2. *The setok is* **not** *online divisible.*

3. *Any share of the setok is* **not** *offline divisible*

4. **No one can go short** *for the setok.*

5. *The setok is T-tradable and the length of the tradable period is given by* $T = \tau_T(t, H(t))$*, where the function* $\tau_T(t,h) : \boldsymbol{R}_+ \times \boldsymbol{R}_+ \to \{0, T_0\}$ *is as follows.*

$$\tau_T(t,h) = \begin{cases} T_0 & \text{if } h > 0 \\ 0 & \text{if } h = 0. \end{cases}$$

   $T_0 > 0$ *is a deterministic constant.*

6. *The setok is T-refundable and the length of the refundable period is given by* $T = \tau_R(t, H(t))$*, where the function* $\tau_R(t,h) : \boldsymbol{R}_+ \times \boldsymbol{R}_+ \to \{0, T_1\}$ *is as follows.*

$$\tau_R(t,h) = \begin{cases} 0 & \text{if } h > 0 \\ T_1 & \text{if } h = 0. \end{cases}$$

   $T_1 > 0$ *is a deterministic constant.*

7. *As long as the up-to-date value $H(t)$ is larger than a threshold value H_θ, each share of the setok gives the holder a dividend whose process is a Poisson process with intensity θ.*
8. *As long as no compromise has occurred, all the up-to-date and implicit value processes are positive and finite.*
9. *Compromise happens according to a Poisson process with intensity λ.*
10. *The setok is compromise-responsive in value.*

The first property $Y(t) = 1$ in Assumption 4.1 implies that the setok is **not** compromise-responsive in price. The intensity θ of the dividend Poisson process represents a total effect of the use of the setok. For example, suppose the setok is a reusable access-grant ticket. The holder feels like using it occasionally, say, with the probability of $\theta_1 dt$ during an infinitesimal time interval. Each use gives him a project value of θ_2. However, the ticket is valid only when the up-to-date value is large enough, say, no smaller than H_θ. Thus, during the infinitesimal time interval $(t, t+dt]$, the dividend is $\theta dt = \theta_1\theta_2 dt$ if $H(t) \geq H_\theta$, and 0 if $H(t) < H_\theta$.

According to Assumption 4.1, we change the assumption on the maturity T_m of the option. In particular, we assume

$$T_m < \min\{T_0, T_1\}. \tag{35}$$

We are interested in the price process of the European call option. The difference from Section 3 in each dynamics is the key for the pricing. The overview is as follows:

Compromise is incorporated into the assumption on the H dynamics of underlying setok.

Non-strict tradability is incorporated both

- into the contribution of one share of the setok to the dynamics of a riskless portfolio (dF)

and

- into the contribution of the option to the dynamics of the riskless portfolio.

Project opportunity is incorporated only into the contribution of one share of the setok to the dynamics of the riskless portfolio.

Now firstly we replace Assumption 3.3 with the following assumption which includes the description of the compromise-responsive value process.

Assumption 4.2 (Continuous-Time Model with Revocation) *In Section 4, we are investigating setok $(S, Y; V, H, n, 1)$ under Assumption 4.1, and the European call option on it. Let $C(t) = c(t, H(t))$ be the price process of the option.*

As an extended continuous-time model, we assume the followings.

- *The function $c(t,h)$ is a $C^{1,2}$-mapping in the domain $\boldsymbol{R}_+ \times \boldsymbol{R}_{++}$, and $c(t,0)=0$ for all $t \in \boldsymbol{R}_+$. $\boldsymbol{R}_{++}$ is the set of positive real numbers.*

- *The dynamics of the up-to-date value process H is given by*

$$dH = (1-\lambda(t,H(t))dt)\,\{\mu(t,H(t))Hdt + \sigma(t,H(t))HdW\} + \lambda(t,H(t))dt\cdot(-H)$$

  where $\mu(t,H(t))$ and $\sigma(t,H(t))$ are adapted processes and W is a Wiener process (under the objective measure). An adapted process $\lambda(t,H(t))$ represents the intensity of the Poisson process. We regard the described revocation risk as a systematic risk (see 5.2).

- *Define $G(t)=\{H(t)\}^{-1}$ and corresponding occurrence as $g=1/h$. We sometimes look at c as a function of t and g. To avoid confusion, we write $\hat{c}(t,g)=c(t,1/g)$, where we assume the function $\hat{c}$ is also a $C^{1,2}$-mapping for $0<g<\infty$.*

- *The price process of the riskless asset is described by the dynamics*

$$dB(t) = r_f B(t)dt$$

  where the short rate r_f is a deterministic constant.

$c(t,0)=0$ suggests that the revocation makes the call option worthless: the holder can no longer sell the option. In addition, if the revocation happens, the payoff at the maturity is zero because of the non-strict tradability; the revocation has ruined the tradability and brought the refundability. Thus we notice that the dynamics of H is given by

$$dH = (\mu-\lambda)Hdt + \sigma HdW. \tag{36}$$

Next, we want to construct a riskless portfolio considering the non-strict tradability and the project opportunity. This will be done in the next subsection 4.3.

4.3 Pricing

As usual, let us consider a riskless portfolio composed of one share of the setok and M options. Let F be the monetary value (in terms of the initial investment at the beginning of the infinitesimal time interval) of this portfolio. As long as no revocation happens, the dynamic strategy tells us to pay

$$F = 1 + MC \tag{37}$$

at the beginning of the infinitesimal time interval. After a revocation, we do not need to price. We want to see dF. Unfortunately, the revocation will not allow g to remain finite; $g \to +\infty$ as $h \to +0$. Therefore, without writing dG like Eqn. (23), we here consider the meaning of Eqn. (27) or equivalently and more instructively Eqn. (28). What we are going to do is to write the expected gain conditioned by the information available at the beginning of the infinitesimal time interval $(t, t+dt]$.

Suppose the up-to-date value is currently large enough for the project: $H(t) \geq H_\theta$. The refundability resulting from the revocation implies that the holder of the setok sells it for the fixed up-to-date price $Y(t) = 1$. So the contribution from one share of the setok to dF in this case (when $H(t) \geq H_\theta$) is

$$(1 - \lambda dt)\Big\{-(\mu - \sigma^2)dt - \sigma dW + \theta dt\Big\} + \lambda dt \cdot 1 = (\lambda + \theta - \mu + \sigma^2)dt - \sigma dW. \tag{38}$$

Unless compromise occurs (this probability is $1 - \lambda dt$), $-(\mu - \sigma^2)dt - \sigma dW$ describes the basic contribution of the (tradability of the) setok given by Eqn. (23)[7]. Also, unless compromise occurs, θdt describes the contribution of the project opportunity which is valid. By contrast, if compromise occurs (this probability is λdt), the holder will get a refund (=the fixed price, 1) but buy nothing; everything will then stop. Also, if compromise occurs, the compromise-responsive value is ruined to be zero and hence smaller than H_θ, which means that there is no contribution of the project opportunity.

Suppose instead that $H(t) < H_\theta$. In this case, we do not have the contribution θdt of the project opportunity. Therefore, the contribution from one share of the setok to dF is

$$(1 - \lambda dt)\Big\{-(\mu - \sigma^2)dt - \sigma dW\Big\} + \lambda dt \cdot 1 = (\lambda - \mu + \sigma^2)dt - \sigma dW. \tag{39}$$

Eqn. (38) and Eqn. (39) can be summarized as

$$\Big\{\lambda + \theta \cdot u\,(H - H_\theta) - \mu + \sigma^2\Big\}\, dt - \sigma dW \tag{40}$$

where we have used a step function $u(h) : \boldsymbol{R} \rightarrow \{0, 1\}$ defined by

$$u(h) = \begin{cases} 1 & (\text{if } h \geq 0) \\ 0 & (\text{otherwise}) \end{cases}. \tag{41}$$

As for the option, we incorporate the effect of the non-strict tradability, *i.e.* $c(t, 0) = 0$, into the dynamics:

$$\begin{aligned} MdC &= M(1 - \lambda dt)\left\{\left(\hat{c}_t - \mu G\hat{c}_g + \sigma^2 G\hat{c}_g + \frac{\sigma^2}{2}G^2\hat{c}_{gg}\right)dt - \sigma G\hat{c}_g dW\right\} \\ &\quad + M\lambda dt \cdot (-\hat{c}) \\ &= M\left(\hat{c}_t - \mu G\hat{c}_g + \sigma^2 G\hat{c}_g + \frac{\sigma^2}{2}G^2\hat{c}_{gg} - \lambda\hat{c}\right)dt - M\sigma G\hat{c}_g dW. \end{aligned} \tag{42}$$

The investigation above (Eqn. (40) and Eqn. (42)) results in

$$\begin{aligned} dF &= \left\{M\left(\hat{c}_t - \mu G\hat{c}_g + \sigma^2 G\hat{c}_g + \frac{\sigma^2}{2}G^2\hat{c}_{gg} - \lambda\hat{c}\right) + \lambda + \theta u(H - H_\theta) - \mu + \sigma^2\right\}dt \\ &\quad - \sigma\left(MG\hat{c}_g + 1\right)dW. \end{aligned} \tag{43}$$

Thanks to the divisibility of the option, by choosing

$$M = -\frac{1}{G\hat{c}_g}, \tag{44}$$

[7] In Eqn. (23), each term is divided by H. This is cancelled out when we divide dG by $G(= 1/H)$ as in Eqn. (26) and in Eqn. (27).

we can make the portfolio risk-free. As usual, M can change over time.

Due to the no-arbitrage requirement, we have

$$\begin{aligned} M\left(\hat{c}_t - \mu G\hat{c}_g + \sigma^2 G\hat{c}_g + \frac{\sigma^2}{2}G^2\hat{c}_{gg} - \lambda\hat{c}\right)& \\ +\lambda + \theta u(H - H_\theta) - \mu + \sigma^2 &= r_f F(t) \\ &= r_f(1 + MC). \end{aligned} \tag{45}$$

Next, we insert Eqn. (44) into Eqn. (45). The resultant relation must hold for any occurrence of the adapted process G as long as no compromise has occurred. So let us use g instead of $G(= 1/H)$ to obtain the following PDE

$$\frac{\sigma^2}{2}g^2\hat{c}_{gg} + \left\{r_f - \lambda - \theta u\left(g^{-1} - H_\theta\right)\right\}g\hat{c}_g - (r_f + \lambda)\hat{c} + \hat{c}_t = 0. \tag{46}$$

We solve this PDE under the boundary condition

$$\hat{c}(T_m, g) = \max\{0, Kg - 1\} \quad (0 < g < \infty). \tag{47}$$

The following theorem gives the summary and remarks.

Theorem 4.1 (Boundary Value Problem under a Revocation Risk) *Let us have Assumption 4.1 for the setok. Consider the European call option defined by Definition 3.1 written on the setok under Assumption 4.2. The maturity of the option is T_m and the strike value is K. $H(t)$ is the up-to-date value process of the setok.*

Then the only pricing function of the form $C(t) = c(t, H(t))$ consistent with the no-arbitrage condition is obtained when

$$c(t,h) = \begin{cases} \hat{c}(t, 1/h) & \text{for } h > 0 \\ 0 & \text{for } h = 0 \end{cases}$$

and $\hat{c}(t, g)$ is the solution of the boundary value problem

$$\frac{\sigma^2}{2}g^2\hat{c}_{gg} + \left\{r_f - \lambda - \theta u\left(g^{-1} - H_\theta\right)\right\}g\hat{c}_g - (r_f + \lambda)\hat{c} + \hat{c}_t = 0$$

$$\hat{c}(T_m, g) = \max\{0, Kg - 1\}$$

in the domain $[0, T_m] \times \boldsymbol{R}_{++}$. $u(h) : \boldsymbol{R} \to \{0, 1\}$ is a step function defined by

$$u(h) = \begin{cases} 1 & (\text{if } h \geq 0) \\ 0 & (\text{otherwise}) \end{cases}.$$

In general, it is difficult to obtain an analytical closed-form solution for the boundary value problem in Theorem 4.1. However, we do not have to be disappointed. We can use numerical approach to obtain approximate solutions. The form of the PDE considered is not too strange.

4.4 Inverse Estimation

Return back to the role of security minister.

Let us see on which parameters the option price obtained from Theorem 4.1 would depend. It does not depend on the drift μ, and the parameters regarding tradability/refundability periods, *i.e.* T_0 and T_1. By contrast, it would depend on the diffusion σ, the maturity date T_m, the short rate r_f, the up-to-date value h, the project parameters (θ and H_θ), and of course the strike value K. In addition, it would depend on λ: the risk of compromise. This suggests that the market data may give you some information on a public opinion about the risk of compromise which has not yet occurred. You want to estimate λ by using the market data observed. This is an inverse problem.

Consider the following procedure for the inverse estimation:

(Procedure 1)

1. By using recent market data excluding option prices, estimate the short rate r_f and the volatility σ of the up-to-date value.
2. Guess the risk of compromise λ.
3. Solve the boundary value problem in Theorem 4.1.
4. Compare the result with recent option price data. If there are a lot of options (on the same setok) with different maturities and/or different exercise values, use them as well. Compute the error of guess, *e.g.* in the least-square's sense. Some weighting may be helpful.
5. If the error is small enough, quit.
6. If you do not satisfied with the error, change the guess and repeat. Typically, if the computed prices are too high, increase the guess. This is an intuitive observation from the fact that a revocation makes the option worthless. Once compromised, one cannot expect any yield from exercising the option and immediately selling (refunding) the setok; that would be just a waste of time.

The boundary value problem may take time to be solved. Procedure 1 in total may be too heavy. But you may be more confident and feel more speedy than in the case of questionnaire.

What you want to do may be just to see whether λ exceeds a certain value, say, λ_0. The intuitive observation tells us that the option price would be lower for larger λ. There is a possibility that the following more practical procedure without repeat will work well.

(Procedure 2)

1. By using recent market data excluding option prices, estimate the short rate r_f and the volatility σ of the up-to-date value.
2. Set $\lambda = \lambda_0$.
3. Solve the boundary value problem in Theorem 4.1.

4. Compare the result with the current option price data. If there are a lot of options (on the same setok) with different maturities and/or different exercise values, use them as well.

5. By using a tool for statistical test, examine whether you can say the computed prices are higher than the observed prices with non-negligible probability.

6. If the answer is Yes, think of it as an alarm. It might be time for you to demonstrate your administrative talent as a minister.

4.5 Effect of Derivatives

This framework is virtual in a sense that there has not been established such a setok world. If we really want to have an option market on the setoks, **we must be careful** about the possible change caused by the introduction of derivatives. Even in the existing finance, the effects of derivatives are on-going theoretical and empirical research topics. There are different opinions.

There is a common public and regulatory perception that derivative securities may increase volatility and can have a destabilizing effect on the underlying market. Basically, they are afraid that poorly informed speculators could have a destabilizing effect. Academic reports on this side are few. A theoretical example is [32] and an empirical example is [33].

Among academic people, however, the opposite opinion has been dominating so far: if derivatives promote information dissemination and collection, introduction of them would reduce volatility. The majority of studies have been in this direction. Examples of theoretical approaches include [34]–[37]. Empirical supports include [38]–[41]. There are also empirical studies which show volatility decreases when the derivatives get more popular in trading quantity [42], [43]. If this is the case for setoks as well, we are happy to introduce derivatives.

Difficulties of this discussion arise, for example, from the followings[44].

- The very first introduction to a particular market is only once.
- There could be a lot of correlation among other assets.
- Regulatory situation can change.

Anyway, it is worth continuing studies.

5 Related Works

5.1 Foreign Derivatives and International Issues

The setok market may seem similar to the foreign exchange market; when we consider tradable single-valued setoks in particular, the ratio of the price to the value can have similar properties to those of foreign exchange rates. The theories of currency and foreign derivatives [45], [46] use different short rates in different countries, which is the major issue of the theory. Foreign currencies are regarded as tradable and divisible assets. This assumption makes the theory easier.

By contrast, our setok framework has been domestic so far; the key point is not in how to deal with the short rate(s) but in how to model the tradability, refundability, and divisibility. Of course, international settings would be very interesting future work. If we assumed that several different virtual currencies are available over the network, the resultant theory would be more interesting: virtually international economy.

As for international issues, there are empirical studies which show that there are common features as well as different features in derivative statistics and questionnaire results among different countries [47]. Common features include

- Major participants in the option market are large firms.
- The highest motivation comes from hedging purposes rather than from speculating and arbitrage.
- The hedging activities are mainly aimed at hedging anticipated transactions within a year.

Different features include

- The highest concern is in the lack of information in some countries, but volatilities in others.
- How popular derivatives are.
- How popular currency derivatives are.

The study of the derivative effect in the setok framework would, if it starts, have to consider differences over countries and regions. Note that even regarding conventional financial derivatives, recently mandated disclosures have just enabled us to obtain a large number of samples to investigate firms' usage of derivatives [48].

5.2 Jump Processes

In the continuous-time model, we derived the PDEs for option pricing based on the no-arbitrage requirement. As far as Section 3, there is nothing to be appended here. However, the model with revocation in Section 4 needs more words here. In particular, about an assumption which is implied by Eqn. (45); in financial words, Eqn. (45) implicitly assumes that the revocation is a *systematic risk*. We mentioned it in Assumption 4.2 but have placed no discussion on it so far.

A related issue is found in the option-pricing theory which allows the underlying stock to have jumps in its price process [19], [21], [49], [50] [8]. They resorted to the conventional CAPM (Capital Asset Pricing Model) [52] by assuming that jump processes describe nonsystematic or idiosyncratic risks, which implies that risks such as firms' defaults have a too wide variety of backgrounds with no good reason to be pre-distributed to appear in

[8] In early days, a study using a sample of NYSE listed common stocks reported that jumps in common stock returns leads relatively small deviations from the Black-Scholes formula [51], which suggests that the bias-elimination by [50] may be insignificant.

a global risk premium. This is an extreme assumption and there are a lot of arguments about the systematic/nonsystematic jump processes [53]–[56]. In fact, jumps observed in stock prices are reported to be systematic across the market portfolio [57], and this phenomenon is more significant in the foreign exchange market than in the stock market [58]. The feature of the foreign exchange and currency option markets can be partly understood by the effect of news arrival [59], [60] and changes in monetary policies [61]. Most of the biases in American foreign currency options appeared consistent with the fact that the underlying spot currency rate follows a mixed jump diffusion process [62]. The mixture of idiosyncratic and systematic jumps is studied in [63], [64]. A more recent study on inefficient index portfolios also supports systematic risks [65], [66]. However, it should be noted that empirical studies are not so easy as one might think. For example, the empirical study on the jump-diffusion process of interest rates has not matured due to the difficulty of likelihood estimation [67], [68]. There are a lot of arguments about CAPM as well [69]–[71] [9].

We have used Eqn. (45), which is based on the systematic case. Heuristically speaking, the more similarly network people or entities look at the revocation risk, the better model our choice of Eqn. (45) would give. In other words, we *hope* that related information is distributed more fairly with less hesitation, and revocation risks shall be more *open* than conventional default risks. This is also an assumption, and we could have neither empirical supports nor objections at present; the setok world has not been established yet. What we can say now is based on a technological insight: our choice could go well with the recent trend in the public-key infrastructure toward a single-directory system [72], [73].

If we can interpret popular information-security software and protocols into a utility function, a conditional-expectation approach would be powerful. The corresponding discussion in finance is in [74], [75] for instance; pricing formulae are derived in a way that the utility function of each investor is optimized. The resultant pricing formula can be expressed by using the conditional expectation operator.

5.3 Credit Derivatives

We introduced a simple example of digital certificate revocation in Section 1. Intuitively, the example reminds us of credit risks[13], [14]. The first issue to be considered in a credit-risk study is how to define credit risk and how to describe an appropriate model. A typical understanding is:

- Credit risk is the risk that an obligor will default in performing its obligations[76].

In our revocation example, the public-key infrastructure (*i.e.* the set of certificate authorities involved) plays a role of an obligor.

How to interpret the word "default" is more difficult in our setok world. This is because not only the revocation of a certificate but also a change of security policies can make a signature unverifiable. Suppose that you have a set of certificates and the public keys of the certificate authorities involved. Suppose also that the system uses a trust

[9] These are nothing but examples; there are really a vast number of studies on utility functions and the CAPM.

metric approach: the signature verification software firstly computes a total trust value of the certificates from the input of trust values written on the certificates. If your security policy allows the final computed trust value, the verification succeeds. Thus not only a change of the certificates but also a change of your policy can cause a verification failure. This is a matter of taxonomy and we believe that our framework can be used in either case.

Recently, an inviting application of credit derivatives is emphasized[77] in finance: to create synthetic assets (*e.g.* credit-linked notes). A portfolio including the option analyzed in Section 4 may be directed to this sort of application. Value/price interpretation functions can contribute to synthetic assets.

An important line of research regarding credit derivatives is the use of transition of ratings[14]. Among a lot of studies, a pricing given in [78] is powerful and pretty much related to our setok modeling. The pricing is based on a continuous-time dynamics for the underlying asset together with rating-dependent coefficients which cause incompleteness. In any case, given the rating and the other input parameters, we can compute the occurrence of the variable described by the dynamics. In the setok world, value/price interpretation functions correspond to this computation procedure.

5.4 Information/Network Security and Economics

Total management of information-security is so hard because of human and social aspects of it. For example, a lot of frauds are resulting from poor motivation for security management. A lot of fear is from financial uncertainty. Even with sufficient technologies (I am not quite sure if such things really are available), most end users cannot understand them. So the very starting point and the very final defense would be interpreted in terms of money and literacy.

In fact, there have been a lot of studies in the interdisciplinary area between information/network security and economics. Let us start with a taxonomy of them: charging, metering, payment, punishment, and insurance. Details are given in the following subsections. Before proceeding to them, it should be noted that there would be more categories if we had a wider view such as *network and economics* rather than *information/network security and economics.*

5.4.1 Charging

In network engineering, Quality-of-Service (QoS) issues are not really new but still actively providing research topics as well as testbeds and projects [6]–[8]. This is because the most common global network, the Internet, is a best-effort network. We may claim a lot of kinds of communication qualities. Most traditional components are bandwidth and reliability. Different QoS levels may be eligible for different prices [5]. Competition among different providers and taxation can make things more complicated [79]. Actual charging policies are not straightforward. This issue is one of the main concerns in Internet economics [80].

Analyses and experiences, both in network engineering and in economics, are required.

5.4.2 Metering

Cost sharing through usage-sensitive pricing or charging can be effective for managing Internet growth [81]. The usage-sensitivity can be either direct or indirect. An Internet Service Provider (ISP) may charge you on the basis of connection duration: how long you keep the Internet connection via the ISP, for instance. This is an example of the direct case. A portal WWW site may charge a company whose advertisement is on the portal page, on the basis of effect: how many visitors click the banner, for instance. This is an example of the indirect case.

In order to implement usage-sensitive pricing, either direct or indirect, we need a secure metering scheme because just a simple record or log may be easily altered; there is a risk of cheating. Efficient solutions for this security problem are not trivial, especially in the case of real-time applications. There have been efforts to do better against this trade-off [82]–[84]. Aiming at more general situation where secure audit log is needed, several protocols have been developed with the help of chains of one-way hashed values [28]–[30]. This research direction of "digital forensics" is important toward dispute settlement in the network society.

This is an area where information-security engineering is applied to support data used in financial transactions.

5.4.3 Payment

When charged, we pay. But how? — We need technologies for payment over an open and insecure network. There are a lot of payment systems. Some assume an underlying infrastructure of financial transaction and settlement, while others assume no other infrastructures.

In the former case, we may use standard protocols which assume an underlying credit-card system. SET (Secure Electronic Transaction) [85] is a good example; it provides confidentiality, reliability, entity authentication, and data integrity needed for the financial data transmission *used* in the credit-card system. It only secures data in transit over an otherwise insecure network.

This is also an area where information-security engineering is applied to support data used in financial transactions.

In the latter case, we may use *digital cash* which is typically a digitally-signed string of a certain format [85]. Actual implementations require more complexity due to the risk that the customer might spend the same digital coin more than once. Usual solutions encode the customer's identity in the coin in a way that the identity is normally protected but is revealed if the customer spends it twice. A typical trick for this is to have a challenge-response protocol between the customer and the merchant when the coin is spent [86]; if the same coin is spent twice, then different challenges have to be answered, which gives away the customer's identity. In terms of cryptographic primitives, blind signature is useful in anonymous payment systems [87]; anyone can check that a stripped signature was formed by using the signer's private key, but the signer knows nothing about the correspondence between the elements of the set of stripped matters and the elements of the set of unstripped matters [88]. It should be noted that the security might rely much on hardware such as smartcards [89], [90] depending on the system design.

The previous paragraph used a word "digital *coin*" which implies that each coin has a fixed monetary value. This is not necessarily true because the technical term has not yet been well defined. What is worth noting here is that

- the system could be more efficient if the monetary value of each coin is less granular [17].

In other words, very discrete digital cash could be more light-weight than almost analogue solutions [10]. The efficiency is more significantly required in some applications: electronic toll collection (ETC) in Intelligent Transportation Systems (ITS), for example [91].

This is an area where information-security engineering is used to construct application systems in finance/economics.

5.4.4 Punishment

A trivial use of punishment mechanism for information security is liability management. If introduced in a proper way, liability can motivate people to manage information security better. I would like to focus on other helpful aspects of punishment in the rest of this subsection.

In a broader sense, information/network security concerns availability as well as confidentiality, authenticity, and integrity. Typical threats to availability are Denial-of-Service (DoS) attacks; an attacker may send plenty of connection requests to a target server in order to exhaust the resource of the target. If the server is an online shopping mall, the attack may not only cause financial damages but also do harm to the reputation of the mall due to the resultant low availability. We dislike an extremely long queue in a supermarket.

To make matters worse, security mechanisms might enhance the DoS threat. Let us suppose a secure handshake before starting a confidential communication. In order to avoid impersonation by intruder-in-the-middle attacks, the handshake protocol is equipped with entity authentication, typically by digital signatures. The signatures shall be verified. Unfortunately, the verification cost is usually expensive in computation, and could be abused by DoS attackers; they launch a lot of bogus requests. The recipient of these requests may be hanged up earlier than in the case of non-secured handshake, because the computational cost or damage per attack is more significant due to the expensive verification. This kind of DoS attack is quite a bitter threat; primitives for a security reduces the resistance against another security property. At the worst case, it could encourage a poor implementation which omits the verification during a busy period.

Intrinsically, we could not make DoS impossible. But we can discourage the attackers by making the attack cost the attacker a great deal. We are happier if the attacker must consume his own computational resource before we consume the same order of our resource. This can be done in several ways [92]–[94]. A quite similar trick is proposed to combat junk e-mails [95], [96]. The common idea is to make the attacks expensive. In other words, attackers are punished by cost. They must invest quite a lot in their resources to launch powerful attacks. Hopefully, the actual budget of them may not allow it.

[10] We say "*very* discrete" and "*almost* analogue" because all the data distributed over a digital communication network are intrinsically discrete.

In a similar line of study, there is a project called *MarketNet* [97] which limits the power of attackers by their virtual budget available. It is assumed that a virtual currency system including a virtual central bank works well for this purpose.

This is an example in which information-security engineering makes use of a common feature of money: we like it and do not want to lose it probably because lack of it may limit activities we want to do.

5.4.5 Insurance

A trivial effect of insurance for information security is people's motivation; better management contributes to lower rate of disasters and thus lower risk premium. I would like to overview another example usage of insurance.

Before we start public-key based secure communication, we must associate the public key confidently with its owner. Because single-authority systems do not scale well in a large network, many systems resort to authentication by a path or chain of authorities [98]–[102]. A single path is weak because it relies on the correctness of all the authorities on the path. Multiple paths may increase assurance but the specific level or value of the assurance may be unclear. Therefore, *trust metrics* for measuring the assurance have been studied by a lot of researchers [9]–[12].

Among them, if we can assume that any damage caused by broken paths can be at least partly compensated by money, an insurance-based approach [104], [4] could absorb miscellaneous fluctuations in the widest range. That approach uses a directed graph model; the nodes are public keys K_j $(j = 1, 2, \cdots)$ and the edge $K_1 \rightarrow K_2$ exists in the graph if the user has a certificate that assigns attributes (including the owner) to K_2 and whose signature can be verified by using K_1. Each edge is labeled with the attributes included in the certificate that the edge represents. Each edge $K_1 \rightarrow K_2$ also has a numeric value that represents an insurance amount; if the private key corresponding to K_2 is compromised and used maliciously, then the owner of K_1 is liable for the stated amount of money. A natural and prudent trust metric in this model would be the minimum insured amount of the name-to-key binding for the target key (Fig. 8). One of the advantages of this metric is its efficiency; the minimum amount can be computed by using well-known efficient maximum-flow algorithms.

We do not intend to discuss pros and cons about this metric here. Instead, we want to point out that there could be similar but different usage of insurance. For example, let us suppose a routing service for a network-security infrastructure which uses identity-based cryptography. In this case, identity-to-address binding could have a similar problem to that in public-key infrastructure, and thus we might think of the use of insurance.

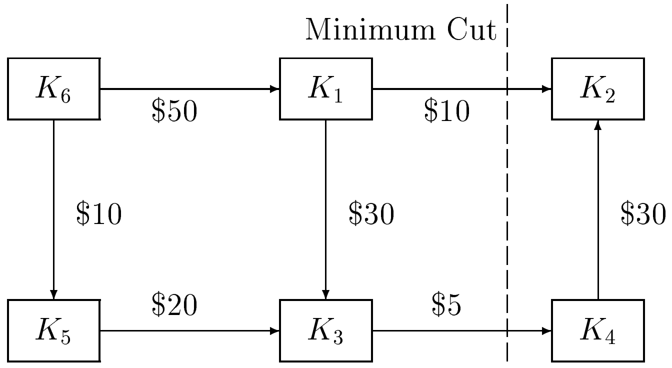

Figure 8: A trust model based on insurance. Each node represents a public key (of a particular owner) the user already have. An edge exists from the node i to the node j if the user has a certificate that assigns attributes to the key K_j and the owner's signature can be verified by using K_i. Each edge has a numeric value that represents an insurance amount; if the private key corresponding to K_2 is compromised and used maliciously, then the owner of K_1 is liable for 10 dollars, for example. A trust metric is defined as the minimum insured amount, which can be computed by using maximum-flow minimum-cut algorithms. In this figure, the minimum is \$10 + \$5 = \$15.

6 Concluding Remarks

6.1 Summary

This framework is an attempt to use stochastic techniques for the future network risk management. We have made an abstraction of uncertain digital objects in network commerce and defined the security token, which is abbreviated into a word coinage *setok*. Each setok has its explicit price, explicit values, and timestamp on it as well as the main contents. A number of properties of the setok were defined. They include value response to compromise, price response to compromise, refundability, tradability, online divisibility, and offline divisibility.

We then investigated a European call option written on the up-to-date value of a setok which has only one explicit value. This setok is called a single-valued setok. In continuous-time as well as discrete-time models, we have derived several option-pricing formulae. These formulae do not require any divisibility of the underlying setok. The basic features of the option price were examined numerically. An intuitive interpretation of the results was given as well.

In search of applications, an inverse estimation of the compromise probability was studied. The result suggests that we may be able to estimate the public opinion about the probability. Finally, the paper shows a wide variety of interdisciplinary surveys in related areas to enrich the implications of our work. These implications as well as the application are quite important for interdisciplinary researchers to try the next stage of this work.

6.2 Setok and Finance/Economics

As mentioned in Section 5, the foreign exchange market is related with this framework. What lies in between is a virtually international and borderless market over the global network. Our setok framework may be extended in that direction. However, we must be careful about the effect of new derivatives in the market. An advanced social science will be needed as well.

The setok framework has investigated only simplified situations so far. A lot of extensions shall be made (and in fact, we have already started some of them):

Untradable and unrefundable setoks: Studies of them may learn a lot from project-investment theory and real options, and vice versa; the abstraction in our framework may contribute to new challenges in the existing areas.

Effect of Short-Selling Restriction: We have derived option-pricing formulae with a restriction that short-selling of the setok is disallowed. In theory, it works. In practice, however, we have to be careful. This is because our financial experiences tell that a short-selling restriction can reduce the informational efficiency of the market [105] [11]. In other words, some of the items in the ideal market assumption (Assumption 3.2) might be threatened. Since we could not have any empirical test at present, a reasonable simulation studies would be helpful.

Other exotic derivatives: In particular, futures are very attractive because

- futures have been most popular in foreign derivatives so far,

and

- most futures are closed before and hence without actual delivery of underlying assets.

6.3 Setok and Information/Network Security

Stochastic approaches are very powerful in studying uncertain social activities. This is what we are facing with in security system engineering. So one possible direction is to use the stochastic technique achieved in the setok study for analyses of information-security systems. An attempt in Section 4 is one of the simplest cases in this direction. Intrusion detection [106]–[114] is another good candidate. To put it in short, studies in this direction are in search of **virtual but reasonable sensors** realized by distributed agents. Setok markets are not necessarily actual economies. If agents make decisions by using a simple set of policies and the sensing/alarm system works well as a whole, it could be regarded as a good application of our setok framework to network security.

Another possible direction is from what the setok world needs. If some setok/option properties could not be realized by the current state of the art in information-security

[11] From January 3rd, 1994, the Stock Exchange of Hong Kong allowed 17 out of 33 constituent stocks of the Hang Seng Index (HSI) to be sold short subject to restrictions. These restrictions were lifted on March 25th, 1996, and at the same time, 113 of the stocks including all the constituent stocks were allowed to be sold short. These relaxations improved the informational efficiency.

engineering, there may be a good opportunity of creating new cryptographic protocols and/or primitives. A flexible timestamping protocol is a good candidate. For example, offline divisibility, which is defined but never used in this paper, would need a timestamp which are secure but allows specified manipulation afterwards.

Finally, we have to point out that how financial tools can help information security. Total management of information-security is so hard because of human and social aspects of it. In fact, a lot of frauds are resulting from poor motivation. A lot of fear is from financial uncertainty. Even with sufficient technologies (I am not quite sure if they really are available), most end users cannot understand them. So the very starting point and the very final defense would be interpreted in terms of money and literacy. By using security-economics approaches based on the setok framework, we are going to enhance motivation and make things easier for people to understand. Financial tools will play a central role there.

References

[1] Bruce Schneier. *Applied Cryptography: protocols, algorithms, and source code in C.* John Wiley & Sons, Inc., 2nd edition, 1996.

[2] J. C. Davis. "Protecting Intellectual Property in Cyberspace". *IEEE Technology and Society Magazine*, Vol. 17, No. 2, pp. 12–25, 1998.

[3] S. Katzenbeisser and F. Petitcolas (eds). *Information Hiding Techniques for Steganography and Digital Watermarking.* Artech House Publishers, Boston, London, 2000.

[4] M. K. Reiter and S. G. Stubblebine. "Authentication metric analysis and design". *ACM Transactions on Information and System Security*, Vol. 2, No. 2, pp. 138–158, May 1999.

[5] R. Edell and P. Varaiya. "Providing Internet Access: What We Learn from INDEX". *IEEE Network*, Vol. 13, No. 5, pp. 18–25, 1999.

[6] X. Xiao and L. M. Ni. "Internet QoS: A Big Picture". *IEEE Network*, Vol. 13, No. 2, pp. 8–18, 1999.

[7] E. W. Knightly and N. B. Shroff. "Admission Control for Statistical QoS: Theory and Practice". *IEEE Network*, Vol. 13, No. 2, pp. 20–29, 1999.

[8] B. Titelbaum, S. Hares, L. Dunn, R. Neilson, V. Narayan, and F. Reichmeyer. "Internet2 QBone: Building a Testbed for Differentiated Services". *IEEE Network*, Vol. 13, No. 5, pp. 8–16, 1999.

[9] U. Maurer. "Modelling a Public-Key Infrastructure". In *Computer Security — ESORICS'96*, Lecture Notes in Computer Science 1146, pp. 325–350, 1996. Springer-Verlag.

[10] D. J. Essin. "Patterns of trust and policy". In *Proc. of New Security Paradigms Workshop '97*, pp. 38–47, September 1997.

[11] M. K. Reiter and S. G. Stubblebine. "Resilient authentication using path independence". *IEEE Trans. Comput.*, Vol. 47, No. 12, pp. 1351–1362, December 1998.

[12] R. Kohlas and U. Maurer. “Confidence valuation in a public-key infrastructure based on uncertain evidence”. In *Proc. of Third International Workshop on Practice and Theory in Public Key Cryptosystems (PKC 2000)*, Lecture Notes in Computer Science 1751, pp. 93–112, January 2000. Springer-Verlag.

[13] G. Dufey and F. Rehm. “An introduction to credit derivatives”. Working Paper 00-013, University of Michigan Business School, January 2001.

[14] V. V. Acharya, S. R. Das, and R. K. Sundaram. “Pricing credit derivatives with rating transitions”. SSRN Working Paper Series, November 2000.

[15] K. Matsuura. “Digital security tokens and their derivatives”. In *7th International Conference of the Society for Computational Economics (SCE’01)*, New Haven, CT, June 2001.

[16] S. Das and R. Sundaram. “A direct approach to arbitrage-free pricing of credit derivatives”. NBER Working Paper Series 6635, National Bureau of Economic Research, July 1998.

[17] T. Eng and T. Okamoto. “Single-term divisible electronic coins”. In *Advances in Cryptology — EUROCRYPT’94*, Lecture Notes in Computer Science 950, pp. 306–319, 1995. Springer-Verlag.

[18] Clifford A. Ball. “Estimation Bias Induced by Discrete Security Prices”. *The Journal of Finance*, Vol. 43, No. 4, pp. 841–865, September 1988.

[19] A. G. Malliaris and W. A. Brock. *Stochastic Methods in Economics and Finance*, Springer: North-Holland, Amsterdam, 1982.

[20] T. E. Copeland and J. F. Weston. *Financial Theory and Corporate Policy.* Addison-Wesley, 3rd edition, 1992.

[21] Robert C. Merton. *Continuous-Time Finance (Revised Edition).* Blackwell Publishers, Cambridge: MA, 1992.

[22] Darrell Duffie. *Dynamic Asset Pricing Theory.* Princeton University Press, Princeton: NJ, 2nd edition, 1996.

[23] Lenos Trigeorgis. *Real Options: Managerial Flexibility and Strategy in Resource Allocation.* MIT Press, Cambridge, 1996.

[24] Tomas Björk. *Arbitrage Theory in Continuous Time.* Oxford University Press, New York, 1998.

[25] J. C. Hull. *Options, Futures, and Other Derivatives.* Prentice-Hall, Upper Saddle River, London, 4th edition, 2000.

[26] S. E. Morris. “Crime and prevention: a Treasury viewpoint”. *IEEE SPECTRUM*, Vol. 34, No. 2, pp. 38–39, February 1997.

[27] Eoghan Casey. *Digital Evidence and Computer Crime — Forensic Science, Computers and the Internet.* Academic Press, 2000.

[28] B. Schneier and J. Kelsey. “Cryptographic support for secure logs on untrusted machines”. In *Proc. of The Seventh USENIX Security Symposium*, pp. 53–62, Berkeley, January 1998.

[29] B. Schneier and J. Kelsey. "Secure audit logs to support computer forensics". *ACM Trans. on Information and System Security*, Vol. 2, No. 2, pp. 159–176, May 1999.

[30] J. Kelsey and B. Schneier. "Minimizing bandwidth for remote access to cryptographically protected audit logs". In *Second International Workshop on the Recent Advances in Intrusion Detection (RAID'99)*, September 1999.

[31] F. Black and M. Scholes. "The pricing of options and corporate liabilities". *Journal of Political Economy*, Vol. 81, pp. 637–654, 1973.

[32] J. C. Stein. "Informational Externalities and Welfare-Reducing Speculation". *Journal of Political Economy*, Vol. 95, No. 6, pp. 1123–1145, December 1987.

[33] L. Harris. "S & P 500 Cash Stock Price Volatilities". *The Journal of Finance*, Vol. 44, No. 5, pp. 1155–1176, December 1989.

[34] J.-P. Danthine. "Information, Futures Prices, and Stabilizing Speculation". *Journal of Economic Theory*, Vol. 17, pp. 79–98, 1978.

[35] S. J. Grossman. "An Analysis of the Implications for Stock and Futures Price Volatility of Program Trading and Dynamic Hedging Strategies". *Journal of Business*, Vol. 61, pp. 275–298, 1988.

[36] J. Detemple and L. Selden. "A general equilibrium analysis of option and stock market interactions". *International Economic Review*, Vol. 32, pp. 279–304, 1991.

[37] H. Henry Cao. "Information acquisition and price behavior in a rational expectations equilibrium". *The Review of Financial Studies*, Vol. 12, No. 1, pp. 131–163, 1999.

[38] F. R. Edwards. "Futures Trading and Cash Market Volatility: Stock Index and Interest Rate Futures". *Journal of Futures Markets*, Vol. 8, pp. 421–440, 1988.

[39] D. J. Skinner. "Options Markets and Stock Return Volatility". *Journal of Financial Economics*, Vol. 23, pp. 61–78, 1989.

[40] J. Conrad. "The Price Effect of Option Introduction". *The Journal of Finance*, Vol. 44, No. 2, pp. 487–498, June 1989.

[41] R. Kumar, A. Sarin, and K. Shastri. "The Impact of Options Trading on the Market Quality of the Underlying Security: An Empirical Analysis". *The Journal of Finance*, Vol. 53, pp. 717–732, 1998.

[42] H. Bessembinder and P. J. Seguin. "Futures-Trading Activity and Stock Price Volatility". *The Journal of Finance*, Vol. 47, No. 5, pp. 2015–2034, December 1992.

[43] H. Bessembinder and P. J. Seguin. "Price Volatility, Trading Volume, and Market Depth: Evidence from Futures Markets". *Journal of Financial and Quantititative Analysis*, Vol. 28, No. 1, pp. 21–39, March 1993.

[44] Jeff Fleming and Barbara Ostdiek. "The impact of energy derivatives on the crude oil market". *Energy Economics*, Vol. 21, pp. 135–167, 1999.

[45] G. S. Lucas. "Interest rates and currency prices in a two-country world". *Journal of Monetary Economics*, Vol. 10, pp. 335–360, 1982.

[46] G. S. Bakshi and Z. Chen. "Equilibrium valuation of foreign exchange claims". *The Journal of Finance*, Vol. 52, pp. 799–826, June 1997.

[47] Per Alkebäck and Niclas Hagelin. "Derivative Usage by Nonfinancial Firms in Sweden with an International Comparison". *Journal of International Financial Management and Accounting*, Vol. 10, No. 2, pp. 105–120, 1999.

[48] Stephen R. Goldberg, Joseph H. Godwin, Myung-Sun Kim, and Charles A. Tritschler. "On the Determinants of Corporate Usage of Financial Derivatives". *Journal of International Financial Management and Accounting*, Vol. 9, No. 2, pp. 132–166, 1998.

[49] R. C. Merton. "On the Pricing of Corporate Debt: The Risk Structure of Interest Rates". *The Journal of Finance*, Vol. 29, pp. 449–470, May 1974.

[50] R. C. Merton. "Option Pricing When Underlying Stock Returns are Discontinuous". *Journal of Financial Economics*, Vol. 3, pp. 125–144, 1976.

[51] Clifford A. Ball and Walter N. Torous. "On Jumps in Common Stock Prices and Their Impact on Call Option Pricing". *The Journal of Finance*, Vol. 40, No. 1, pp. 831–842, March 1985.

[52] William F. Sharpe. "Capital Asset Prices: A Theory of Market Equilibrium under Conditions of Risk". *The Journal of Finance*, Vol. 19, No. 3, pp. 425–442, September 1964.

[53] Chang Mo Ahn and Howard E. Thompson. "Jump-Diffusion Processes and the Term Structure of Interest Rates". *The Journal of Finance*, Vol. 43, No. 1, pp. 155–174, March 1988.

[54] Vasanttilak Naik and Moon Lee. "General equilibrium pricing of options on the market portfolio with discontinuous returns". *Review of Financial Studies*, Vol. 3, No. 4, pp. 493–521, 1990.

[55] Chang Mo Ahn. "Option pricing when jump risk is systematic". Working Paper, Michigan State University, 1991.

[56] David B. Colwell and Robert J. Elliott. "Discontinuous asset prices and non-attainable contingent claims". *Mathematical Finance*, Vol. 3, No. 3, pp. 295–308, July 1993.

[57] Robert A. Jarrow and Eric R. Rosenfeld. "Jump risks and the intertemporal capital asset pricing model". *Journal of Business*, Vol. 57, No. 3, pp. 337–351, July 1984.

[58] P. Jorion. "On jump processes in the foreign exchange and stock markets". *Review of Financial Studies*, Vol. 1, No. 4, pp. 427–445, 1988.

[59] M. Mussa. "Empirical regularities in the behavior of exchange rates and theories of the foreign exchange market". *Carnegie-Rocbester Conference on Public Policy*, Vol. 11, pp. 9–57, 1979.

[60] Jacob A. Frenkel. "Flexible Exchange Rates, Prices, and the Role of "News": Lessons from the 1970s". *Journal of Political Economy*, Vol. 89, No. 4, pp. 665–705, August 1981.

[61] Robert P. Flood and Robert J. Hodrick. "Asset Price Volatility, Bubbles, and Process Switching". *The Journal of Finance*, Vol. 41, No. 4, pp. 831–842, September 1986.

[62] James N. Bodurtha Jr. and Georges R. Courtadon. "Tests of American Option Pricing Model on the Foreign Currency Option Market". *Journal of Financial and Quantitative Analysis*, Vol. 22, No. 2, pp. 153–167, June 1987.

[63] Kaushik I. Amin and Victor K. Ng. "Option valuation with systematic stochastic volatility". *The Journal of Finance*, Vol. 48, No. 3, pp. 881–910, July 1993.

[64] Kaushik I. Amin. "Jump diffusion option valuation in discrete time". *The Journal of Finance*, Vol. 48, No. 5, pp. 1833–1863, December 1993.

[65] D. Ashton and M. Tippett. "Systematic risk and empirical research". *Journal of Business Finance & Accounting*, Vol. 25, pp. 1325–1356, 1998.

[66] I. Garrett. "Discussion of systematic risk and empirical research". *Journal of Business Finance & Accounting*, Vol. 25, pp. 1357–1362, 1998.

[67] N. D. Pearson and T. S. Sun. "Exploiting the Conditional Density in Estimating the Term Structure: An Application to the Cox, Ingersoll, and Ross Model". *The Journal of Finance*, Vol. 49, No. 4, pp. 1279–1304, 1994.

[68] Bing-Huei Lin and Shih-Kuo Yeh. "Jump-Diffusion Interest Rate Process: An Empirical Examination". *Journal of Business Finance & Accounting*, Vol. 26, pp. 967–995, 1999.

[69] Ravi Jagannathan and Zhenyu Wang. "The Conditional CAPM and the Cross-Sections of Expected Returns". *The Journal of Finance*, Vol. 51, No. 1, pp. 3–53, March 1996.

[70] Eugene F. Fama and Kenneth R. French. "Multifactor Explanations of Asset Pricing Anomalies". *The Journal of Finance*, Vol. 51, No. 1, pp. 55–84, March 1996.

[71] Eugene F. Fama and Kenneth R. French. "The CAPM is Wanted, Dead or Alive". *The Journal of Finance*, Vol. 51, No. 5, pp. 1947–1958, December 1996.

[72] A. Buldas, P. Laud, and H. Lipmaa. "Accountable certificate management using undeniable attestations". In *Proc. of 7th ACM Conference on Computer and Communication Security*, pp. 9–18, November 2000.

[73] I. Gassko, P. S. Gemmell, and P. MacKenzie. "Efficient and fresh certification". In *Proc. of Third International Workshop on Practice and Theory in Public Key Cryptosystems (PKC 2000)*, Lecture Notes in Computer Science 1751, pp. 342–353, January 2000. Springer-Verlag.

[74] N. Bouleau and D. Lamberton. "Residual Risks and Hedging Strategies in Markovian Markets". *Stoch. Proc. and Appl.*, Vol. 33, pp. 131–150, 1989.

[75] D. Lamberton and B. Lapeyre. *Introduction to Stochastic Calculus Applied to Finance.* Chapman & Hall, Cambridge: MA, 1996.

[76] P. U. Ali. "e-Credit Derivatives: Buying and Selling Credit Risk over the Internet". *Journal of Banking & Finance Law and Practice*, Vol. 12, June 2001.

[77] P. U. Ali. "New Applications for Credit Derivatives". *Company and Securities Law Journal*, Vol. 19, , August 2001.

[78] V. Brunel. "Pricing credit derivatives with uncertain default probabilities". SSRN Working Paper Series, January 2001.

[79] R. M. Dewan, M. L. Freimer, and A. Seidmann. "Internet Service Providers, Proprietary Content, and the Battle for Users' Dollars". *Communications of the ACM*, Vol. 41, No. 8, pp. 43–48, August 1998.

[80] Lee W. McKnight and Joseph P. Bailey. "An introduction to internet economics". In Lee W. McKnight and Joseph P. Bailey, editors, *Internet Economics*, pp. 3–24, Cambridge, Massachusetts, 1997. MIT Press.

[81] N. Brownlee. "Internet pricing in practice". In Lee W. McKnight and Joseph P. Bailey, editors, *Internet Economics*, pp. 77–90, Cambridge, Massachusetts, 1997. MIT Press.

[82] M. K. Franklin and D. Malkhi. "Auditable Metering with Lightweight Security". In *Pre-Proceedings of Financial Cryptography'97*, pp. 1–9, February 1997.

[83] M. Naor and B. Pinkas. "Secure and efficient metering". In *Advances in Cryptology — EUROCRYPT'98*, Lecture Notes in Computer Science 1403, pp. 576–590, 1998. Springer-Verlag.

[84] M. Naor and B. Pinkas. "Secure Accounting and Auditing on the Web". *Computer Networks and ISDN Systems*, pp. 541–550, 1998.

[85] M. A. Sirbu. "Credits and debits on the Internet". *IEEE SPECTRUM*, Vol. 34, No. 2, pp. 23–29, February 1997.

[86] T. Okamoto and K. Ohta. "Disposable zero-knowledge authentications and their applications to untraceable electronic cash". In *Advances in Cryptology — CRYPTO'89*, pp. 481–496, Lecture Notes in Computer Science 435, 1990. Springer-Verlag.

[87] D. Chaum and S. Brands. "Minting electronic cash". *IEEE SPECTRUM*, Vol. 34, No. 2, pp. 30–34, February 1997.

[88] D. Chaum. "Blind signatures for untraceable payments". In *Advances in Cryptology: Proceedings of Crypto 82*, pp. 199–203, 1983. Plenum Press.

[89] C. H. Fancher. "In your pocket: smartcards". *IEEE SPECTRUM*, Vol. 34, No. 2, pp. 47–53, February 1997.

[90] G. Horn and B. Preneel. "Authentication and payment in future mobile systems". In *Proc. of ESORICS'98*, Lecture Notes in Computer Science 1485, pp. 277–293, 1998. Springer-Verlag.

[91] G. Hanaoka, T. Nishioka, Y. Zheng, and H. Imai. "An Optimization of Credit-Based Payment for Electronic Toll Collection Systems". *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E83-A, No. 8, pp. 1681–1690, August 2000.

[92] K. Matsuura and H. Imai. "Protection of authenticated key-agreement protocol against a denial-of-service attack". *Cientifíca*, Vol. 2, No. 11, pp. 15–19, September 1998.

[93] A. Juels and J. Brainard. "Client Puzzles: A Cryptographic Defense Against Connection Depletion Attacks". In *Proc. of NDSS'99 (Networks and Distributed Security Systems)*, pp. 151–165, 1999.

[94] K. Matsuura and H. Imai. “Modified Aggressive Modes of Internet Key Exchange Resistant against Denial-of-Service Attacks”. *IEICE Transactions on Information and Systems*, Vol. E83-D, No. 5, pp. 972–979, May 2000.

[95] C. Dwork and M. Naor. “Pricing via processing or combatting junk mail”. In *Advances in Cryptology — CRYPTO’92*, Lecture Notes in Computer Science 740, pp. 139–147, August 1993. Springer-Verlag.

[96] C. Dwork and M. Naor. “Pricing via processing or combatting junk mail”. Technical Report CS95-20, Faculty of Mathematical Sciences, The Weizmann Institute of Science, 1995.

[97] Y. Yemini, A. Dailianas, D. Florissi, and G. Huberman. “MarketNet: Market-Based Protection of Information Systems”. In *Proceedings of First International Conference on Information and Computation Economies (ICE’98)*, Charleston, SC, October 1998.

[98] J. J. Tardo and K. Alagappan. “SPX: Global Authentication Using Public Key Certificates”. In *Proceedings of the 1991 IEEE Symposium on Research in Security and Privacy*, pp. 232–244, May 1991.

[99] S. Kent. “Internet Privacy Enhanced Mail”. *Communications of the ACM*, Vol. 36, No. 8, pp. 48–60, August 1993.

[100] P. R. Zimmermann. *The Official PGP User’s Guide.* MIT Press, 1995.

[101] D. W. Chadwick, A. J. Young, and N. K. Cicovic. “Merging and extending the PGP and PEM trust models — the ICE-TEL trust model”. *IEEE Network*, Vol. 11, No. 3, pp. 16–24, June 1997.

[102] R. Perlman. “An Overview of PKI Trust Models”. *IEEE Network*, Vol. 13, No. 6, pp. 38–43, November 1999.

[103] A. Abdul-Rahman and S. Hailes. “A distributed trust model”. In *Proc. of New Security Paradigms Workshop ’97*, pp. 48–60, September 1997.

[104] M. K. Reiter and S. G. Stubblebine. “Toward acceptable metrics of authentication”. In *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, pp. 10–20, May 1997.

[105] J. K. W. Fung and L. Jiang. “Restrictions on short-selling and spot-futures dynamics”. *Journal of Business Finance & Accounting*, Vol. 26, pp. 227–248, 1999.

[106] D. Denning. “An intrusion-detection model”. *IEEE Transactions on Software Engineering*, Vol. 13, No. 2, pp. 222–232, February 1987.

[107] S. Cheung and K. N. Levitt. “Protecting routing infrastructures from denial of service using cooperative intrusion detection”. In *Proc. of New Security Paradigms Workshop ’97*, pp. 94–106, September 1997.

[108] S. Wu, F. Wang, B. Vetter, W. Rance Cleaveland II, Y. Jou, F. Gong, and C. Sargor. “Intrusion detection for link-state routing protocols”. In *5-minute talk in the 1997 IEEE Symposium on Security and Privacy*, May 1997.

[109] R. P. Lippmann, R. Cunningham, D. Fried, S. Garfinkel, G. A. I. Graf, K. Kendall, D. McClung, D. Weber, S. Webster, D. Wyschogrod, and M. Zissmann. "MIT Lincoln Laboratory Offline Component of DARPA 1998 Intrusion Detection Evaluation". `http://ideval.ll.mit.edu`, December 1998. DARPA PI Meeting slides.

[110] S. Elbaum and J. C. Munson. "Intrusion detection through dynamic software measurement". In *Proc. of Workshop on Intrusion Detection and Network Monitoring (ID'99)*, pp. 41–50, April 1999.

[111] A. K. Ghosh, A. Schwartzbard, and M. Schatz. "Learning program behavior profiles for intrusion detection". In *Proc. of Workshop on Intrusion Detection and Network Monitoring (ID'99)*, pp. 51–62, April 1999.

[112] M. Gupta and M. Subramanian. "Preprocessor algorithm for network management codebook". In *Proc. of Workshop on Intrusion Detection and Network Monitoring (ID'99)*, pp. 93–102, April 1999.

[113] L. Girardin. "An eye on network intruder-administrator shootouts". In *Proc. of Workshop on Intrusion Detection and Network Monitoring (ID'99)*, pp. 19–28, April 1999.

[114] J. B. D. Cabrera, B. Ravichandran, and R. K. Mehra. "Statistical traffic modeling for network intrusion detection". In *Proc. of the 8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS 2000)*, pp. 466–473, August 2000.