IPSJ Transactions on Mathematical Modeling and Its Applications Vol. 3 No. 3 107–116 (Oct. 2010)

Regular Paper

Towards Modeling Stored-value Electronic Money Systems

Shunsuke Inenaga,[†1] Kenichiro Oyama[†1]
and Hiroto Yasuura[†1]

This paper presents mathematical and general models of electronic money systems. The goal of the paper is to propose a first framework in which various kinds of e-money systems can be uniformly represented and their security properties can be evaluated and compared. We introduce two kinds of e-money system models; a *note-type e-money system model* and a *balance-type e-money system model*. We show that any balance-type e-money system with efficient data transmission cannot be simulated by any note-type e-money system. This implies that balance-type e-money systems are strictly faster in data communication. Then, we show that a forged monetary value can be detected in some note-type e-money systems, while it cannot be detected in any balance-type e-money systems with efficient data communication. This implies that note-type e-money systems seem to be more secure.

1. Introduction

Electronic money (*e-money*) is a new kind of money that is stored and spent only electronically. In particular, stored-value e-money systems have been successful and widely used in countries such as Japan, Hong-Kong, and Singapore, due to their convenience. In these systems, an electronic monetary value is stored on a device that is controlled by a user, such as a smart card and a mobile phone. Stored-value e-money systems are often used as an efficient replacement of cash payments with coins and notes, because users do not have to look for coins and notes in their wallet and merchants do not have to store many coins and notes for changes. Also, since most stored-value e-money systems employ contact-less smart cards as users' devises, payments can very quickly be done simply by facing a smart card to a card reader.

Two types of stored-value e-money systems are popular today; One is a *note-type* e-money system in which digital notes are stored within each user's devise (e.g., a smart card). Since note-type e-money systems are electronic simulation of today's physical cash systems, the value of each digital note is fixed. The first note-type e-money was proposed by Chaum [1] (called electronic cash or e-cash therein), and it has extensively been studied since (e.g., see Refs. 2)–6)). An example of a real-world note-type e-money system is a British e-money system called mondex [7]. The other is a *balance-type* e-money system in which an accumulated value representing the balance of money is stored within each user's devise. Prepaid e-money systems that have widely been used in Japan, Hong-Kong, and Singapore are kinds of balance-type e-money system.

Most e-money systems currently used in the real world are of the latter type, balance-type e-money systems [8]. This is because balance-type e-money systems tend to be much more "lightweight" than note-type ones. Indeed, this paper will show that what distinguishes note-type and balance-type e-money systems is the data size communicated between users for money value exchanges. That is, we will prove that the lower bound of data size for a value transfer in any note-type e-money system is strictly larger than that in any balance-type e-money system.

Security and privacy properties of stored-value e-money systems have been well studied [9], and there have been some attempts to analyze different kinds of stored-value e-money systems from security and privacy viewpoints [10),11]. However, the existing researches have not provided any general framework in which various e-money systems can be compared in a uniform way, or any analysis of security and privacy in a unified manner. Motivated by this background, this paper presents a first mathematical and general model for stored-value e-money systems. All the existing stored-value e-money systems well fit into our model, and hence we can compare their security properties within a unified framework.

In this paper, we analyze security properties of e-money systems with *off-line payments* [5], where neither a trusted third party or the bank is involved in any e-money transfer between users. That is, the users' devises are assumed to be capable of peer-to-peer communications (e.g., infrared ray communication between two mobile phones, or a contact-less smart card and a card reader). In particular, this paper focuses on the *detectability of forged monetary values*. This is a rather important security issue of e-money, as it is easy to duplicate

†1 Graduate School of Information Science and Electrical Engineering, Kyushu University

or alter electronic data. We analyze the detectability of forged values in note-type and balance-type e-money systems, based on the proposed general e-money models. As a result, we will show that some note-type e-money systems have detectability of forged values, while no balance-type e-money systems with an efficient communication complexity have the detectability.

The rest of the paper is organized as follows. In Section 2, we introduce a general money system model which consists of three kinds of elements: holders, mediums, and values. Examples of holders are wallets for cash systems and smart cards for e-money systems. Mediums can be seen as (digital and physical) coins and notes. Values represent monetary values (e.g., 1 dollar, 2 dollars, etc.) of mediums. Sections 3 and 4 extend the general money model to a note-type e-money system model and to a balance-type e-money system model, respectively. In Section 5, we introduce *lightweight protocols* for e-money transfer between holders. The concept of lightweight protocols differentiates note-type and balance-type e-money systems in terms of communication data efficiency. In Section 6, we show detectability (resp. undetectability) of forged values in note-type e-money systems (resp. balance-type e-money systems). Finally in Section 7 we conclude and state our future work.

A preliminary version of this paper is in Ref. 12).

2. Money System Model

In this section, we present our general money system model and some operations on the proposed model. A money system is formalized as follows.

Definition 1 *A money system is a quintuple* $(V, M, H, \mathtt{vf}, \mathtt{hf})$ *such that*

- $V = \{0, 1, 2, \ldots, n\}$ *is a finite set of non-negative integer values,*
- M *is a finite set of mediums,*
- H *is a finite set of holders,*
- $\mathtt{vf} : M \to V$ *is called a value function, and*
- $\mathtt{hf} : M \to H$ *is called a holder function.*

A medium m is an abstract model of anything that represents a monetary value v. A coin and a note are examples of a medium. A holder is an abstract model of anything or anyone that stores a medium. A wallet and a smart card are examples of a holder, and a user himself can also be regarded as a holder.

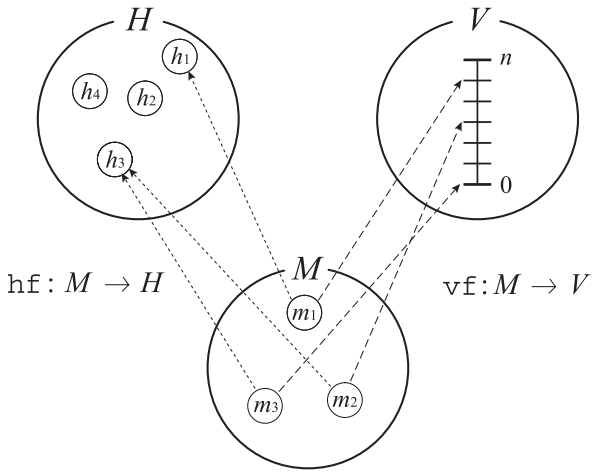

Fig. 1 The money system model. The arrows from M to H represent the $\mathtt{hf}$ function, while those from M to V do the $\mathtt{vf}$ function.

For any $m \in M$, if $h = \mathtt{hf}(m) \in H$, then we say that holder h has medium m. For any $m \in M$, if $v = \mathtt{vf}(m) \in V$, then we say that medium m carries value v. For any $h \in H$, if $v = \sum_{\mathtt{hf}(m)=h} \mathtt{vf}(m) \in V$, then we say that holder h has total value v.

Figure 1 shows the money system model of Definition 1.

Example. Assume that holder `Alice` has a 1 dollar coin c. Then $\mathtt{hf}(c) = \mathtt{Alice}$ and $\mathtt{vf}(c) = 1$.

In the following subsections, we introduce *operations* by a holder or by a pair of holders, which will extend the above static model to a dynamic one. Each operation makes some alteration to the mapping $\mathtt{vf}$ from M to V and/or to the mapping $\mathtt{hf}$ from M to H. To distinguish the mappings before and after an operation, we introduce the notion of time unit t. We denote by $\mathtt{vf}^t$ and $\mathtt{hf}^t$ the mappings $\mathtt{vf}$ and $\mathtt{hf}$ at time t, respectively. After an operation has been conducted, the resulting mappings are denoted by $\mathtt{vf}^{t+1}$ and $\mathtt{hf}^{t+1}$, respectively. That is, a single operation increases the time unit by one.

2.1 Money Transfer

A most basic operation in the money system model is to transfer some amount

of money (value) from a holder to another holder, which is formalized as follows.

Definition 2 *A transfer of value $v \in V$ from holder $h \in H$ to holder $h' \in H$ $(h \neq h')$ at time t is an operation such that*

$$\sum_{\mathtt{hf}^t(m)=h} \mathtt{vf}^t(m) \geq v, \tag{1}$$

$$\sum_{\mathtt{hf}^{t+1}(m)=h} \mathtt{vf}^{t+1}(m) = \sum_{\mathtt{hf}^t(m)=h} \mathtt{vf}^t(m) - v, \tag{2}$$

$$\sum_{\mathtt{hf}^{t+1}(m)=h'} \mathtt{vf}^{t+1}(m) = \sum_{\mathtt{hf}^t(m)=h'} \mathtt{vf}^t(m) + v, \tag{3}$$

and for any holder $h'' \neq h, h'$,

$$\sum_{\mathtt{hf}^{t+1}(m)=h''} \mathtt{vf}^{t+1}(m) = \sum_{\mathtt{hf}^t(m)=h''} \mathtt{vf}^t(m). \tag{4}$$

Equation (1) implies that a transfer of value v can be conducted only if the total values that holder h has is at least v. Eq. (2) implies that the total values that holder h has decreases by v, and Eq. (3) does that the total values that holder h' has increases by v. Eq. (4) says that the total values that any other holder h'' has does not change due to the transfer.

Example. Assume that `Alice` has a total of 10 dollars and `Bob` has a total of 5 dollars at time t. Now `Alice` is giving 4 dollars to `Bob`. Then $\sum_{\mathtt{hf}^t(m)=\mathtt{Alice}} \mathtt{vf}^t(m) = 10$, $\sum_{\mathtt{hf}^t(m)=\mathtt{Bob}} \mathtt{vf}^t(m) = 5$, $\sum_{\mathtt{hf}^{t+1}(m)=\mathtt{Alice}} \mathtt{vf}^{t+1}(m) = 10 - 4 = 6$, and $\sum_{\mathtt{hf}^{t+1}(m)=\mathtt{Bob}} \mathtt{vf}^{t+1}(m) = 5 + 4 = 9$.

Remark. The money model of Definition 1 lacks the *bank*, an important entity of money systems. However, we can regard the bank as a special kind of holder in our model. A *withdrawal* of money is then regarded as a value transfer from the bank to a holder, and a *deposit* of money is the other way round.

2.2 Money Forgery

Next, we define an operation that relates to an attack to the system. Let $\mathtt{fvf} : M \to V$ be a function called a *forged value function*. We assume that $\mathtt{fvf}^t(m) \geq \mathtt{vf}^t(m)$ for any medium $m \in M$ and at any time t.

Definition 3 *A forgery of value $fv > 0$ by holder $h \in H$ at time t is an operation such that*

$$\mathtt{fvf}^{t+1}(m) = \mathtt{vf}^t(m) + fv \text{ and} \tag{5}$$

$$\mathtt{vf}^{t+1}(m) = \mathtt{vf}^t(m) \tag{6}$$

with some medium $m \in M$ such that $\mathtt{hf}^t(m) = \mathtt{hf}^{t+1}(m) = h$.

Equations (5) and (6) imply that although the value measured by the forged value function `fvf` of medium m increases by fv from time t to time $t+1$, the actual value by the value function `vf` does not change from time t to time $t+1$. The above value fv is called a *forged value*.

Example. Assume that `Alice` has a smart card s with the balance of 1 dollar at time t, and now she is illegally adding a forged value of 9 dollars into her smart card. Then $\mathtt{fvf}^{t+1}(m_s) = \mathtt{vf}^t(m_s) + fv = 1 + 9 = 10$, where m_s denotes a medium associated with the smart card s.

2.3 Forged Money Transfer

Next we define an operation of transferring a forged value from a holder to another holder.

Definition 4 *A transfer of forged value $fv \in V$ from holder $h \in H$ to holder $h' \in H$ $(h \neq h')$ at time t is an operation such that*

$$\sum_{\mathtt{hf}^t(m)=h} \mathtt{fvf}^t(m) \geq \sum_{\mathtt{hf}^t(m)=h} \mathtt{vf}^t(m) + fv, \tag{7}$$

$$\sum_{\mathtt{hf}^{t+1}(m)=h} \mathtt{fvf}^{t+1}(m) = \sum_{\mathtt{hf}^t(m)=h} \mathtt{fvf}^t(m) - fv, \tag{8}$$

$$\sum_{\mathtt{hf}^{t+1}(m)=h'} \mathtt{fvf}^{t+1}(m) = \sum_{\mathtt{hf}^t(m)=h'} \mathtt{fvf}^t(m) + fv, \tag{9}$$

and for any holder $h'' \neq h, h'$,

$$\sum_{\mathtt{hf}^{t+1}(m)=h''} \mathtt{fvf}^{t+1}(m) = \sum_{\mathtt{hf}^t(m)=h''} \mathtt{fvf}^t(m). \tag{10}$$

Equation (7) implies that a transfer of forged value fv can be conducted only if the total forged values that holder h has is at least fv. Eq. (8) implies that the total forged values that holder h has decreases by fv, and Eq. (9) does that the total forged values that holder h' has increases by fv. Eq. (10) says that the total forged values that any other holder h'' has does not change due to the transfer.

Example. Assume that holder `Alice` has a fake 10 dollar note b, and is giving b to

Bob. Since $\mathtt{fvf}^t(b) = 10$, we get $\sum_{\mathtt{hf}^t(m)=\mathtt{Alice}} \mathtt{fvf}^t(m) - \sum_{\mathtt{hf}^t(m)=\mathtt{Alice}} \mathtt{vf}^t(m) \geq \mathtt{fvf}^t(b) - \mathtt{hf}^t(b) = 10$, $\sum_{\mathtt{hf}^{t+1}(m)=\mathtt{Alice}} \mathtt{fvf}^{t+1}(m) = \sum_{\mathtt{hf}^t(m)=\mathtt{Alice}} \mathtt{fvf}^t(m) - 10$, and $\sum_{\mathtt{hf}^{t+1}(m)=\mathtt{Bob}} \mathtt{fvf}^{t+1}(m) = \sum_{\mathtt{hf}^t(m)=\mathtt{Bob}} \mathtt{fvf}^t(m) + 10$.

2.4 (Un)detectability of Forged Money

We define the *detectability* of a forged value, as follows.

Definition 5 *A forged value $fv \in V$ w.r.t. medium $m \in M$ is said to be detectable at time t if $\mathtt{fvf}^t(m) - \mathtt{vf}^t(m) = fv$ is computable (under some conditions), and is said to be undetectable otherwise.*

In this paper, we deal with the following problem that concerns the security of money systems.

Problem 1 (Detectability of transferred forged value) *Assume that forged value $fv > 0$ is transferred from any holder $h \in H$ to any holder $h' \in H$ $(h \neq h')$ at time t. Is forged value fv detectable at time $t + \alpha$ with $\alpha \geq 1$?*

In Sections 3 and 4 we will introduce two kinds of e-money systems based on the money model of Definition 1. Section 5 will discuss the significant difference between those systems. Then in Section 6 we will discuss Problem 1 for the two kinds of e-money systems.

3. Note-Type E-Money System Model

In this section, we propose a *note-type* e-money system model that is an electronic simulation of today's note-based cash system. This type of e-money system has been in practical use [13] and has widely been studied [1)–6)].

Definition 6 *An note-type e-money system is a money system of Definition 1 with the following restriction: For any medium $m \in M$ and at any time t,*

$$\mathtt{vf}^{t+1}(m) = \mathtt{vf}^t(m). \tag{11}$$

That is, in a note-type e-money system model, the value that each medium carries is fixed (i.e., invariant with time), as is the case with the physical cash system.

Definition 7 *A transfer of value $v \in V$ from holder h to holder h' $(h \neq h')$ in a note-type e-money system is an operation such that for some $Q \subseteq M$,*

$$\mathtt{hf}^t(m) = h \quad \text{for any } m \in Q,$$
$$\sum_{m \in Q} \mathtt{vf}^t(m) = v,$$

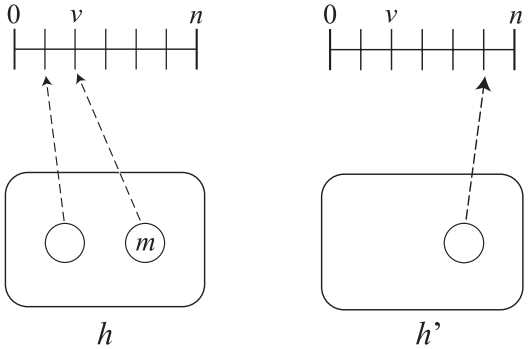

Fig. 2 Before transferring value v from h to h' on a note-type e-money system at time t. There exists medium m such that $\mathtt{vf}^t(m) = v$ and $\mathtt{hf}^t(m) = h$.

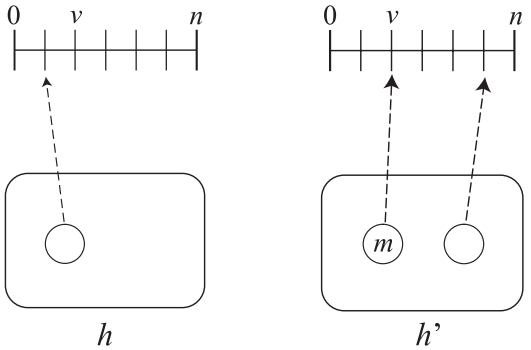

Fig. 3 After transferring value v from h to h' on a note-type e-money system at time $t + 1$. Now $\mathtt{vf}^{t+1}(m) = v$ and $\mathtt{hf}^{t+1}(m) = h'$. Also $\mathtt{hf}^{t+1}(m') = \mathtt{hf}^t(m')$ for any $m' \neq m$.

$$\mathtt{hf}^{t+1}(m) = h' \quad \text{for any } m \in Q,$$

and for any $m' \notin Q$, $\mathtt{hf}^{t+1}(m') = \mathtt{hf}^t(m')$.

See **Fig. 2** and **Fig. 3** that illustrate a transfer of value v from h to h' in a note-type e-money system model.

The following proposition shows that a money transfer of a note-type e-money system defined above is a money transfer of a money system model.

Proposition 1 *A transfer of value $v \in V$ in a note-type e-money system of*

Definition 7 satisfies the conditions of Definition 2.

Proof. $\sum_{m\in Q} \mathtt{vf}^t(m) = v$ satisfies Condition (1). By Eq. (11), $\sum_{m\in Q} \mathtt{vf}^{t+1}(m) = v$ after a transfer of value v. Moreover, since $\mathtt{hf}^t(m) = h$, $\mathtt{hf}^{t+1}(m) = h'$ for any $m \in Q$, and $\mathtt{hf}^{t+1}(m') = \mathtt{hf}^t(m')$ for any $m' \notin Q$, we get $\sum_{\mathtt{hf}^{t+1}(m)=h} \mathtt{vf}^{t+1}(m) = \sum_{\mathtt{hf}^t(m)=h} \mathtt{vf}^t(m) - v$, $\sum_{\mathtt{hf}^{t+1}(m)=h'} \mathtt{vf}^{t+1}(m) = \sum_{\mathtt{hf}^t(m)=h'} \mathtt{vf}^t(m) + v$, and for any holder $h'' \neq h, h'$, $\sum_{\mathtt{hf}^{t+1}(m)=h''} \mathtt{vf}^{t+1}(m) = \sum_{\mathtt{hf}^t(m)=h''} \mathtt{vf}^t(m)$. Hence Conditions (2), (3), and (4) hold. □

Now we define a forged value transfer in a note-type e-money system as follows:

Definition 8 *A transfer of forged value $fv \in V$ from holder h to holder h' ($h \neq h'$) in a note-type e-money system is an operation such that for some $R \subseteq M$,*

$$\mathtt{hf}^t(m) = h \quad \text{for any } m \in R,$$
$$\sum_{m\in R} \mathtt{fvf}^t(m) = \sum_{m\in R} \mathtt{vf}^t(m) + fv,$$
$$\mathtt{hf}^{t+1}(m) = h' \quad \text{for any } m \in R,$$
$$\sum_{m\in R} \mathtt{fvf}^{t+1}(m) = \sum_{m\in R} \mathtt{vf}^{t+1}(m) + fv,$$

and for any $m' \notin R$, $\mathtt{hf}^{t+1}(m') = \mathtt{hf}^t(m')$.

Proposition 2 *A transfer of forged value $fv \in V$ in a note-type e-money system of Definition 8 satisfies the conditions of Definition 4.*

Proof. Since $\mathtt{hf}^t(m) = h$ for any $m \in R$ and $\sum_{m\in R} \mathtt{fvf}^t(m) = \sum_{m\in R} \mathtt{vf}^t(m) + fv$, Condition (7) is satisfied. Since $\mathtt{hf}^{t+1}(m) = h' \neq h$ for any $m \in R$, we have that

$$\{p \in M \mid \mathtt{hf}^{t+1}(p) = h\} = \{q \in M \mid \mathtt{hf}^t(q) = h\} - R \quad \text{and}$$
$$\{p' \in M \mid \mathtt{hf}^{t+1}(p') = h'\} = \{q' \in M \mid \mathtt{hf}^t(q') = h'\} \cup R.$$

Therefore Conditions (8) and (9) hold. Condition (10) holds since $\mathtt{hf}^{t+1}(m') = \mathtt{hf}^t(m')$ for any $m' \notin R$. □

4. Balance-Type E-Money System Model

Here, we propose a *balance-type* e-money system model in which an accumulated value that represents the balance of money is stored in each holder. That is, a fixed single medium is associated with each holder, and the value that is carried by the medium varies with time. A number of balance-type e-money systems have been proposed and are in practical use[8].

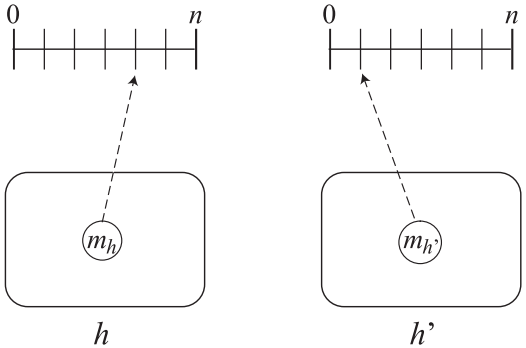

Fig. 4 Before transferring value v from h to h' on a balance-type e-money system at time t. Here we have $\mathtt{vf}^t(m_h) \geq v$.

Definition 9 *A balance-type e-money system is a money system of Definition 1 with the following restriction: At any time t, $\mathtt{hf}^t$ is a bijection and for any $m \in M$*

$$\mathtt{hf}^t(m) = \mathtt{hf}^{t+1}(m).$$

Namely, in the balance-type e-money system model, there is a one-to-one relation between a holder and a medium, and the relation is invariant over time.

For any holder $h \in H$, let m_h denote a unique medium that h has, namely $\mathtt{hf}^t(m_h) = h$.

A transfer of value in a balance-type e-money system is defined as follows:

Definition 10 *A transfer of value $v \in V$ from holder $h \in H$ to holder $h' \in H$ ($h \neq h'$) in a balance-type e-money system is an operation such that*

$$\mathtt{vf}^t(m_h) \geq v,$$
$$\mathtt{vf}^{t+1}(m_h) = \mathtt{vf}^t(m_h) - v,$$
$$\mathtt{vf}^{t+1}(m_{h'}) = \mathtt{vf}^t(m_{h'}) + v,$$

and for any $m' \in M$ such that $m' \neq m_h$ and $m' \neq m_{h'}$, $\mathtt{vf}^{t+1}(m') = \mathtt{vf}^t(m')$.

See **Fig. 4** and **Fig. 5** that illustrate a transfer of value v from holder h to another holder h' in the balance-type e-money system model.

The following proposition shows that a money transfer of the balance-type e-money system defined above is a money transfer of a money system model.

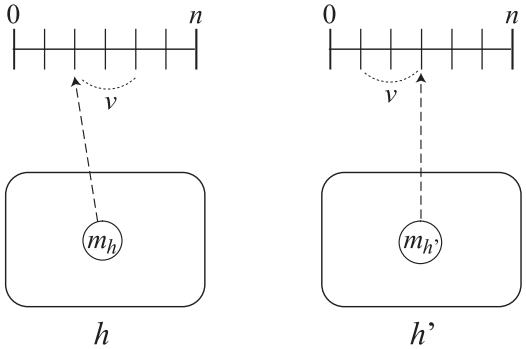

Fig. 5 After transferring value v from h to h' on a balance-type e-money system at time $t+1$. Now $\mathtt{vf}^{t+1}(m_h) = \mathtt{vf}^t(m_h) - v$ and $\mathtt{vf}^{t+1}(m_{h'}) = \mathtt{vf}^t(m_{h'}) + v$.

Proposition 3 *A transfer of value $v \in V$ in a balance-type e-money system of Definition 10 satisfies the conditions of Definition 2.*

Proof. Since $\mathtt{hf}^t$ is a bijection and $\mathtt{hf}^t(m_h) = h$ for any holder $h \in H$, we have $\sum_{\mathtt{hf}^t(m)=h} \mathtt{vf}^t(m) = \mathtt{vf}^t(m_h)$ for any time t. Hence the proposition holds. □

A transfer of forged value in a balance-type e-money system is defined as follows:

Definition 11 *A transfer of forged value $fv \in V$ from holder $h \in H$ to holder $h' \in H$ $(h \neq h')$ in a balance-type e-money system is an operation such that*

$\mathtt{fvf}^t(m_h) \geq \mathtt{vf}^t(m_h) + v$,
$\mathtt{fvf}^{t+1}(m_h) = \mathtt{fvf}^t(m_h) - v$,
$\mathtt{fvf}^{t+1}(m_{h'}) = \mathtt{fvf}^t(m_{h'}) + v$,

and for any $m' \in M - \{m_h, m_{h'}\}$, $\mathtt{fvf}^{t+1}(m') = \mathtt{fvf}^t(m')$.

Proposition 4 *A transfer of forged value $fv \in V$ in a balance-type e-money system of Definition 11 satisfies the conditions of Definition 4.*

Proof. Since $\mathtt{hf}^t(m_h) = h$ and $\{m \in M \mid \mathtt{hf}^t(m) = h\} = \{m_h\}$ for any holder h and time t, Conditions (7), (8), and (9) hold. Condition (10) holds since $\mathtt{vf}^{t+1}(m') = \mathtt{vf}^t(m')$ and $\mathtt{fvf}^{t+1}(m') = \mathtt{fvf}^t(m')$ for any $m' \in M - \{m_h, m_{h'}\}$. □

5. Lightweight Money Transfer Protocol

In this section, we introduce *lightweight* protocols for transferring a value in the e-money systems of the previous sections. A lightweight protocol is a protocol that transmits minimum amount of data for a value transfer between holders.

Definition 12 *Any protocol for a transfer of a value from holder h to holder h' is said to be lightweight if it satisfies the following properties:*

(a) The protocol is "off-line". That is, the communication is only between h and h' and neither the bank or a trusted third party is involved in the protocol.
(b) The data transmitted from one holder to the other is at most $\lceil \log_2 n \rceil + O(1)$ bits.

Lightweight protocols are basic, yet useful to construct practical e-money systems, as a value transfer between holders can quickly be accomplished. Also, since the data communication is off-line and only between holders, anonymous payments are possible with lightweight protocols.

It is not difficult to see that there exist lightweight protocols for a balance-type e-money system, which satisfy the properties of Definition 12. For instance, consider the following protocol in which a value v is transferred from holder h to holder h' in a balance-type e-money system.

(1) Holder h sends integer v to holder h'.
(2) Holder h subtracts v from the value in medium m_h.
(3) Holder h' adds v to the value in medium $m_{h'}$.
(4) Holder h' tells holder h that h' has received v.

It is rather clear that the communication of the above protocol is only between h and h'. Also, as the value of v is at most n, we can transfer value v using $\lceil \log_2 n \rceil$ bits.

Note that we can encrypt the value v by common-key or public-key encryption algorithms without increasing its data size, hence lightweight protocol can protect its communication contents from eavesdroppers.

It is also possible to extend the above protocol so that the two holders conduct mutual authentication: We can index each holder h_i using an id i for each holder. Each id can be implemented with $\lceil \log_2 |H| \rceil$ bits. Assuming that H is fixed and the length of credentials (e.g., passwords) is linear in $\lceil \log_2 |H| \rceil$ or is constant, h

and h' can mutually authenticate each other while only constant-sized data are communicated between them. We remark that in most of real-world applications the length of credentials is constant.

On the other hand, the following lemma shows that a value transfer in any note-type e-money system cannot be implemented by a lightweight protocol.

Lemma 1 *A value transfer in any note-type e-money system requires to transmit data of size* $\Omega(n^{\frac{1}{3}} \log n)$ *from holder* h *to holder* h'.

Proof. Consider k distinct values $1 \leq n_1 < n_2 < \cdots < n_k \leq n$. Let x be the maximum number of mediums that the holder h has for every value n_i, where $1 \leq i \leq k$. Then there exist $(x+1)^k$ combinations of mediums that the holder h may have. Therefore at least $\lceil \log_2(x+1)^k \rceil = \lceil k \log_2(x+1) \rceil$ bits of information is required to be transmitted from holder h to holder h'.

Let n be the maximum value that can be transferred between holders. If $n_k = n^{\frac{1}{3}}$, then

$$\frac{xk(2n^{\frac{1}{3}} - k + 1)}{2} = \frac{x(2kn^{\frac{1}{3}} - k^2 + k)}{2} \leq n.$$

Now consider the case $(x(2kn^{\frac{1}{3}} - k^2 + k))/2 = n$. Choosing $k = n^{\frac{1}{3}}$, we get $x = O(n^{\frac{1}{3}})$. Hence $\lceil k \log_2(x+1) \rceil = O(n^{\frac{1}{3}} \log n)$ bits of information is required to be transmitted from h to h' in this case.

We finally remark that the preconditions of a value transfer in a note-type e-money system of Definition 7 are all satisfied in the above scenario. □

Lemma 1 also means that a lightweight value transfer protocol is what distinguishes note-type e-money systems from balance-type e-money systems, that is, any balance-type e-money systems with a lightweight protocol cannot be simulated by any note-type e-money systems.

6. (Un)detectability of Forged Values

In this section we show whether a forged value is detectable or undetectable in e-money systems, after a forged value transfer of Definition 8 or Definition 11 has conducted.

Recall Problem 1 that defines the problem of detecting a forged value fv that has been transferred from holder h to holder h'. In the sequel, we consider the following specific situation:

- At time t, holder h' has value zero, that is,

$$\sum_{\mathtt{hf}^t(m)=h'} \mathtt{vf}^t(m) = \sum_{\mathtt{hf}^t(m)=h'} \mathtt{fvf}^t(m) = 0.$$

- A value $v > fv$ is transferred from holder h to holder h' at time t.

The first assumption is to simplify the analysis. The second assumption is to make the problem more interesting, difficult, and realistic – a mixture of (legal) value and forged value is transferred from holder h to holder h', and the task is to compute how much out of the mixed value has been forged.

Theorem 1 *There exists a note-type e-money system in which the forged value* fv *is detectable.*

Proof. We here deal with the case where a single medium carrying value v is transfered from holder h to holder h'. The cases where more than one medium are transferred can be shown similarly.

Now consider the following note-type e-money system: Each medium m_j is assigned a unique index j, with $1 \leq j \leq |M|$. Each holder has an array A of size $|M|$ such that $A[j]$ stores the value of medium m_j, that is, $A[j] = \mathtt{vf}(m_j)$. By definition of a note-type e-money system, the value of each element $A[j]$ is fixed for any time t. Assume that the value of a medium m_j has been forged and it is transferred from h to h' at time t. Let $fv = \mathtt{fvf}^t(m_j) - \mathtt{vf}^t(m_j) = v - \mathtt{vf}^t(m_j) > 0$. Then fv is detectable since $A[j] = \mathtt{vf}^{t+\alpha}(m_j) = \mathtt{vf}^t(m_j)$ for $\alpha \geq 1$. Using a public-key digital signature algorithm (e.g., see Ref. 14)), we can check whether the index j of a medium m_j has been illegally altered or not.

Let us now consider a duplicated medium dm from some medium m such that $\mathtt{vf}^t(m) = v$. Note $fv = \mathtt{fvf}^t(dm) - \mathtt{vf}^t(dm) = v - 0 = v$. This cannot be solved simply by using the array A. However, it has been shown in the literature (e.g., see Ref. 4)) that it is possible to construct a note-type e-money system in which every duplicated medium dm can be detected by the bank after dm is sent from h to h'. We remark that the bank is only contacted by holder h' after a transaction between the holders. Hence any value transfer between holders remains off-line. Therefore the theorem holds. □

As shown above, the forged value is detectable in some note-type e-money system. On the contrary, the following theorem shows that the forged value is

undetectable in any balance-type e-money system which uses a lightweight value transfer protocol.

Theorem 2 *In any balance-type e-money system, the forged value fv is undetectable with a lightweight value transfer protocol of Definition 12.*

Proof. Note that, by Lemma 1, we cannot apply Theorem 1 to any balanced-type e-money system using a lightweight protocol.

Let $r = v - fv$ and d be the function s.t. $d(v, r) = v - r = fv$. Then the problem of detecting the forged value fv is identical to computing the value $d(v, r)$.

We prove the theorem by showing that the one-way deterministic communication complexity [15] from h to h' so that the value $d(v, r)$ is computable is $2\lceil \log_2 n \rceil$ bits. Let us denote the communication complexity by C. Recall that the maximum possible value for v is n. Since the value v is already transfered from h to h', and h' did not know the value v beforehand, the communication complexity C is at least $\lceil \log_2 n \rceil$. Hence the question is how large is the extra data that need to be additionally transmitted from h to h' in order that $d(v, r)$ is computable.

We regard computing $d(v, r)$ as determining the cell (v, r) of an $n \times (n + 1)$ matrix D such that $D[i, j] = i - j$ for $1 \leq i \leq n$ and $0 \leq j \leq n$. As was shown in Ref. 15), the one-way communication complexity is $\lceil \log_2(drow(D)) \rceil$ bits, where $drow(D)$ denotes the number of distinct rows in D. Since $D[i+1, j] = D[i, j]+1$ for every $1 \leq i \leq n-1$, we have $drow(D) = n$. Therefore, $C \geq \lceil \log_2 n \rceil + \lceil \log_2(drow(D)) \rceil = \lceil \log_2 n \rceil + \lceil \log_2 n \rceil = 2\lceil \log_2 n \rceil$. On the other hand, it can easily be seen that $C \leq 2\lceil \log_2 n \rceil$. Hence $C = 2\lceil \log_2 n \rceil$.

By Definition 12, the data transmitted from h to h' in any lightweight protocol must be at most $\lceil \log_2 n \rceil + O(1)$ bits. Hence we conclude that the forged value fv is undetectable in any balance-type e-money systems that employ a lightweight protocol. □

7. Conclusions and Future Work

This paper presented a general model of money systems and its extended versions to two kinds of e-money systems, note-type and balance-type e-money systems. Using the notion of a lightweight protocol, we showed that balance-type e-money systems are more efficient than note-type e-money systems in terms of the data size transmitted between holders. On the other hand, we showed that note-type e-money systems are more secure than balance-type e-money systems from the view point of detectability of forged values.

The results of this work suggest the followings:

(1) In a balance-type e-money system, the upperbound n for a monetary value transfer has to be kept small. This is because once a large forged monetary value is mixed with a legal value, it cannot be detected due to Theorem 2. Also, it is suggested that a balance-type e-money system in the real world should be limited to closed-loop payments, that is, once an electronic monetary value is used for purchase, it cannot be directly reused and has to be changed to cash. This suggestion also comes from undetectability of forged values shown in Theorem 2.

(2) A note-type e-money system may become a "next-generation" secure e-money system. However, a drawback of this type of e-money system is that a merchant (a holder that receives money) needs to store enough "changes" for arbitrary monetary value transfer, like today's physical cash systems. This obviously spoils a benefit of electronic payments.

According to the above discussions, our future work is to model the following type of e-money system: A divisible e-cash system [16),17)] allows an electronic coin to be divided into two coins having the same total amount of values as the original coin. This allows us exact and efficient payments without using changes. Divisible e-cash systems can be seen as an intermediate between note-type e-money systems and balance-type e-money systems. A divisible e-cash system can be described using our money model of Definition 1, as follows. Any medium m having a value $v \geq 2$ at time t can be divided into two mediums m_1 and m_2 having values $v_1 \geq 1$ and $v_2 \geq 1$, respectively, with $v_1 + v_2 = v$. That is, $\mathtt{vf}^t(m) = v$ and and $\mathtt{vf}^{t+1}(m_1) + \mathtt{vf}^{t+1}(m_2) = v_1 + v_2 = v$. The detectability of forged values in divisible e-cash systems needs to be examined using our model.

Yamasaki, et al. [18)] proposed a general model of door access control that is based on finite state machines. In their model, a door-key is regarded as a medium that represents the right of a user to open a door, and various types of door-keys such as physical keys, card keys, passwords, and biometrics well fit into the model. The inherent difference between door-access control and e-money systems is whether each medium takes a Boolean value or a non-negative integer

value. This implies that it should be possible to extend the model of Ref. 18) to e-money systems, and this may lead us to further insight of e-money systems.

Acknowledgments This work was in part supported by the Research Superstar Program of Kyushu University and by grant 08-01 from the Okawa Foundation for Information and Telecommunications.

References

1) Chaum, D.: Blind Signatures for Untraceable Payments, *CRYPTO'82*, pp.199–203, Plenum Press (1982).
2) Au, M.H., Susilo, W. and Mu, Y.: Practical Compact E-Cash, *ACISP'07*, LNCS, Vol.4586, pp.431–445, Springer (2007).
3) Brands, S.: Untraceable Off-line Cash in Wallet with Observers, *CRYPTO'93*, LNCS, Vol.773, pp.302–318, Springer (1993).
4) Camenisch, J., Hohenberger, S. and Lysyanskaya, A.: Compact E-Cash, *EUROCRYPT'05*, LNCS, Vol.3494, pp.302–321, Springer (2005).
5) Chaum, D., Fiat, A. and Naor, M.: Untraceable Electronic Cash, *CRYPTO'88*, LNCS, Vol.403, pp.319–327, Springer (1988).
6) Gouget, A.: Recent Advances in Electronic Cash Design, *CARDIS'08*, LNCS, Vol.5189, pp.290–293, Springer (2008).
7) Mondex. http://www.mondex.com/
8) Payment and Settlement Systems Department, Bank of Japan: Recent Developments in Electronic Money in Japan (2008). BOJ Reports & Research Papers (Oct. 2008).
9) Hanacek, P.: Security of Electronic Money, *Proc. SOFSEM'98*, LNCS, No.1521, pp.107–121 (1998).
10) Miyazaki, S. and Sakurai, K.: Classification of Off-line Electronic Money Systems and Evaluation of the Security against Insider Attacks (in Japanese), *Transactions of Information Processing Society of Japan*, Vol.40, No.3, pp.1294–1304 (1999).
11) Suzuki, M. and Hirokawa, K.: Security Analysis on Electronic Money Systems Including Compromise of Cryptographic Algorithms and/or Devices (in Japanese), *IEICE Technical Report*, ISEC, No.2008-69, pp.39–46 (2008).
12) Inenaga, S., Oyama, K. and Yasuura, H.: Towards Modeling Stored-Value Electronic Money Systems, *CISIM'09*, pp.902–907, IEEE Computer Society (2009).
13) Clemons, E.K., Croson, D.C. and Weber, B.W.: Reengineering Money: the Mondex Stored Value Card and Beyond, *International Journal of Electronic Commerce*, Vol.1, No.2, pp.5–31 (1996).
14) Schneier, B.: *Applied Cryptography*, Wiley (1996).
15) Yao, A.C.-C.: Some Complexity Questions Related to Distributed Computing, *STOC'79*, pp.209–213, ACM (1979).
16) Canard, S. and Gouget, A.: Divisible E-Cash Systems Can Be Truly Anonymous, *EUROCRYPT'07*, LNCS, Vol.4515, pp.482–497, Springer (2007).
17) Okamoto, T.: An Efficient Divisible Electronic Cash Scheme, *CRYPTO'95*, LNCS, Vol.963, pp.438–451, Springer (1995).
18) Yamasaki, T., Inenaga, S., Ikeda, D. and Yasuura, H.: Modeling Costs of Access Control with Various Key Management Systems, *PDPTA'09*, pp.676–682, CSREA Press (2009).

(Received January 8, 2010)
(Revised May 11, 2010)
(Accepted July 5, 2010)

Shunsuke Inenaga is an associate professor of Institute for Advanced Study, Kyushu University, and is a research associate professor of Graduate School of Information Science and Electrical Engineering, Kyushu University. He received his B.E. from Kyushu Institute of Technology in 2000, and his M.S. and Ph.D. in science from Kyushu University in 2002 and 2003, respectively. He became a research associate professor of Kyushu University in 2006, and an associate professor of Institute for Advanced Study, Kyushu University in 2009. His current research interests include stringology, algorithms and data structures, and design and modeling of social information infrastructure. He is a member of IPSJ and EATCS.

Kenichiro Oyama received his B.E. and M.E. from Kyushu University in 2005 and 2007, respectively. His research interest includes modeling electronic money systems. He currently works for Fusic CO., Ltd.

Hiroto Yasuura is an executive vice president of Kyushu University. He is also a professor of Department of Computer Science and Communication Engineering, Graduate School of Information Science and Electrical Engineering, and a member of System LSI Research Center in Kyushu University. Prof. Yasuura received his B.E., M.E. and Ph.D. degrees in computer science from Kyoto University, Kyoto, Japan, in 1976, 1978, and 1983 respectively. He was an associate professor in Kyoto University and moved to Kyushu University in 1991. His current interests include embedded system design, hardware/software co-design, system design methodology and social infrastructure. He is a fellow of IEICE and IPSJ.