General Model for Secure Electronic Cash Scheme

Dany Eka Saputra[1], Sarwono Sutikno[2], and Suhono Harso Supangkat[2]
(Corresponding author: Dany Eka Saputra)
Departement on Informatics, STMIK "AMIKBANDUNG"[1]
Jl. Jakarta no 28, Kota Bandung, Jawa Barat, Indonesia
School of Electrical Engineering, Institut Teknologi Bandung[2]
Jl. Ganesha No 10, Kota Bandung, Jawa Barat, Indonesia
(Email: dekastra@gmail.com)
(Received Nov. 01, 2017; Revised and Accepted June 18, 2018; First Online Feb. 24, 2019)

Abstract

The vast variation of electronic cash scheme make it difficult to compare a scheme with another. We propose a general model of electronic cash. The development of the model uses logical modeling based on Inenaga *et al.* model of money system. The model consists of three submodel: the model of system, the model of process, and the model of property. The model of system describe the basic model of electronic cash data, entity, and form. The model of process enlist the common process found in electronic cash scheme. The model of property describes the common property in electronic cash scheme, including security property. We find that our model can be used as a base of security evaluation and covers wider variation of electronic cash scheme than the model in Inenaga *et al.*

Keywords: Electronic Cash; Mathematic Modeling; Security Model

1 Introduction

Comparing and choosing electronic cash schemes for an implementation requires great effort. Each scheme need to be reviewed to list its respective properties and choose the one that suits the implementation. However, two different schemes may define a single property differently. This condition may complicate the effort to define the security objectives of electronic cash and may hamper the security of the implementation. For example, Dreier *et al.* proposed a method to evaluate the security of electronic cash [9]. The works of Chen & Chou [7], and Wang *et al.* [28] also attempt to evaluate another existing schemes. However, the definition of forgery in [9] differs with the definition used in [7] and [28].

An attempt to design new electronic cash scheme face similar problem. Different definition of property and behavior may lead to incorrect design. This condition may result in insecure scheme. Having standard definition or model of electronic cash and its property (including security property) greatly help the process of designing a new scheme or comparing schemes for implementation.

Modeling a common definition of electronic cash demands quite an effort. A model usually represents certain aspect of an object. By observing the object for any pattern that represent the object's properties, we can build a model of the object. In electronic cash, extracting those pattern is a challenging task. Due to the numerous scheme of electronic cash, we can find many variation of property and its definition. Under this condition, it is difficult to extract a common pattern. For a start, the electronic cash scheme can be divided into two paradigms: centralized and distributed electronic cash [26]. Both paradigms have different ways to describe and process electronic cash. Cannard-Gouget [2] explain four definition of anonymity, which is differs from the definition of anonymity in most of electronic cash scheme.

Inenaga *et al.* propose a model of money system [15]. The model describes the general model of money system that can be used to model electronic cash. The model also describes the transfer model of electronic cash and the security property of electronic cash. However, the model only covers off-line electronic scheme. It does not model the electronic cash data creation process and does not consider the issuer of electronic cash as part of the system. The model lacks the generality needed to describe electronic cash system.

We propose a new General Model of Electronic Cash. We take several concepts from Inenaga *et al.* and form a new model that covers wider range of electronic cash scheme. The model is build by using logical approach, so it can be used as a tool to design new scheme or to compare and evaluate existing scheme.

The proposed model only covers the description of centralized electronic cash. By using this paradigm, we refer electronic cash as a digital representative of cash that cre-

ated after exchanging a certain amount of cash to the electronic cash issuer. Distributed electronic cash (or cryptocurrency), such as Bitcoin [22], can not be described by using our model. The hybrid (centralized-distributed) electronic cash scheme ([8, 14, 20, 27]) also cannot be described using our model.

The rest of this paper is arranged as follows. Next, we will describe the definition of electronic cash data and system. The third part of this paper explains the model of process in electronic cash. The next part contains the property of electronic cash, including security property. We give a case study where we use our model to analyze the security of Chaum's Untraceable Electronic Cash scheme [6]. We also compare our model with Inenaga *et al.* model at the end of this paper.

2 Model of Electronic Cash System

2.1 Electronic Cash Data

The model starts with the definition of electronic cash data. The definition acts as the basis of the rest of the model. The definition of electronic cash data is as follows.

Definition 1. *Let m be a medium to store monetary value, v is a non-negative integer represents denomination of monetary value, and u is the owner's identity of a money. An electronic cash data e is defined as a function of m, v, and u, such as:*

$$e = f(m, v, u).$$

In [15], a medium is mapped to a value and the holder/owner of the electronic cash. The value function (vf) is a function that maps a medium to a value. The holder function (hf) is a mapping of a medium to a holder. We take this concept from [15] and redefine the function as follows.

Definition 2. *Given a certain medium m and a single denomination value v, where $v \in \mathbb{Z} \wedge v > 0$, a value function is defined as a function of m and v, declared as*

$$vf_m^v = f(m, v).$$

The value function bonds a medium and a value, enables the determination of the value of electronic cash and the authenticity of monetary value upon evaluation. The holder function is defined as follows.

Definition 3. *For a certain medium m and an owner of electronic cash u, a holder function is a mapping function of a medium to a holder. This notion is declared as:*

$$hf_m^u = f(m, u).$$

The holder function represents proof of ownership of an electronic cash data. Any entity can define the ownership of an electronic cash by using the holder function. By using Definition 2 and Definition 3, we can redefine the definition of electronic cash data (from Definition 1) as

$$e = f(vf_m^v, hf_m^u). \tag{1}$$

The rest of the model uses Equation (1) as reference to electronic cash data. Equation (1) implies that an electronic cash data must, at least, consist of two data: Value function and holder function.

2.2 Electronic Cash System

The sub-model of electronic cash system describes the entities, the processes of electronic cash, and the relationship between entities and processes. First, we need to define the entities in electronic cash system. In most of the schemes such as in [4] and [6], the schemes involve three entities. However, there are schemes which involve more entities (such as [23]) or less [3].

In this model, we model the entities as a set. There are four entities in the set. The role in electronic cash system defines each entity. We describe the model of entity as follows.

Definition 4. *Let E be a set of entity in an electronic cash scheme. The set of E is defined as*

$$E = \{P, U, I, R\},$$

where:

- *P is a single principal that manage and arbitrate the entire system,*
- *I is an issuer of electronic cash,*
- *U is a finite set of electronic cash user/holder, where $U = u_1, u_2, \ldots, u_i, \forall i \in \mathbb{Z}^+$,*
- *R is a finite set of electronic cash merchant/receiver, where $R = r_1, r_2, \ldots, r_j, \forall i \in \mathbb{Z}^+$.*

It is possible for a P and I to be implemented as a single entity. This can be seen in [19]. Although in [18] there seems to exist separate I and P, both original signer and proxy signer can be considered as the same entity with the responsibility of both I and P.

The processes of electronic cash defines how the system works. Each process involves one or more entities. We define the model of process as a set of processes as follows.

Definition 5. *Let A be a set of action/process related to electronic cash system. The membership of A is defined as:*

$$A = \{\texttt{SETUP}, \texttt{CREATE}, \texttt{SPEND}, \texttt{DEPOSIT}, \texttt{ARBITRATE}\},$$

where:

- `SETUP` *is a process to generate system parameters, including entity's credential,*

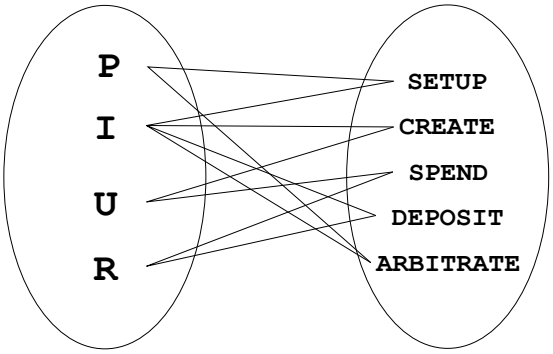

Figure 1: The mapping of electronic cash system

- `CREATE` *is a process to generate electronic cash data* e,
- `SPEND` *is a process to use an electronic data* e *in a transaction,*
- `DEPOSIT` *is a process to settle electronic cash data usage,*
- `ARBITRATE` *is a process to settle a dispute regarding electronic cash usage.*

The processes in Definition 5 represent the general process of an electronic cash system. It only describes the processes directly linked to electronic cash system's life cycle [5]. A scheme may implement more process, such as in [3]. However, these extra process are usually a sub process of a process in A.

Interaction between entities and process related to electronic cash is a general definition of electronic cash system. By referring to Definition 4 and Definition 5, we can redefine the general definition as "*a set of entities conduction a set of processes to use electronic cash data*". This definition can uses a simple mapping as its model, as shown in Figure 1. The formal definition of electronic cash system can be defined as follows.

Definition 6. *An electronic cash system* $\hat{e}$ *is a many-to-many mapping from set* E *to set* A *over finite amount of electronic cash data*

$$\hat{e} : E \to A.$$

2.3 Electronic Cash Form

The Definition 1 and Equation (1) define the data of electronic cash. However, the implementation method of value function determines the form of e-cash. In scheme such as [16], each e has a single denomination value, that will not change throughout its life cycle. Different approach is taken by some scheme, such as [4]. The value of e can change during its life cycle.

The first case the value function is constant. The value function will not change on a transaction, even when the holder function changed. The form which implements this method is defined as *fix-valued electronic cash*. The definition of this form is defined as:

Definition 7. *Let* v_a *be a constant that represent a denomination, where* $v_a \in \mathbb{Z}^+$, *and* m_a *is a single unique medium which holds* v_a. *A fix-valued electronic cash is a system of* $\hat{e}$ *that satisfy:*

$$vf_{m_a}^{m_a} = f(m_a, v_a) = constant$$

for any n `SPEND` *operation.*

The second case of implementation changes the electronic cash value function but usually retain its holder function. This form of electronic cash can be defined as *variable-valued electronic cash*. The formal definition is as follows.

Definition 8. *For a given medium* m_a, *a variable-valued electronic cash is a system of* $\hat{e}$ *that satisfy:*

$$vf_{m_a}^{v} = vf_{m_a}^{v_1} + vf_{m_a}^{v_2} + \ldots + vf_{m_a}^{v_n}$$

or

$$vf_{m_a}^{v} = f(m_a, v(n))$$

where n *is any number of* `SPEND` *operation, and* $v_1, v_2, \ldots, v_n \in \mathbb{Z}^+$.

3 Model of Electronic Cash Processes

The sub model of electronic cash processes defines the models of each process in Definition 5. The model contains the algorithm of each process. This algorithm explain how to conduct each process in general terms. The implementation of this model may contains more steps and protocols, depends on the underlying cryptographic scheme or mechanics in the implementation.

3.1 SETUP Process

`SETUP` is a process to create a set of parameters as a basis of the entire system operation. The process involves P, I, or $u \in U$ to cooperate and create the parameters. The parameters could be in form of modulus, public-private key pair, or other value. The model of this process is as follows.

Definition 9. *For each entity* i, *where* $i \in E$, `SETUP` *is an algorithm to create a set of variables* $a_i = \{a_{i1}, a_{i2}, \ldots, a_{in}\}$ *as* i*'s parameters in system* $\hat{e}$. *Algorithm 1 explains this process.*

3.2 CREATE Process

`CREATE` defines the process of electronic cash withdrawal. In many schemes, the process is called withdraw process. This paper uses 'create' as this process name to emphasis the process of data creation.

Algorithm 1 SETUP Algorithm

1: Begin
2: i contacts P and request for admission in $\hat{e}$.
3: P calculates a_i.
4: P sends a_i to i.
5: i keeps a_i.
6: End

Definition 10. *For each $u \in U$,* CREATE *is a process to request an electronic cash data e with value of v from I by using steps explained in Algorithm 2.*

Algorithm 2 CREATE Algorithm

1: Begin
2: u choose a medium m_u.
3: u create a request in form of $r_e = f(a_u, m_u, v)$ and send it to I.
4: I calculate $vf^v_{m_u}$, $hf^u_{m_u}$, and $e = f(vf^v_{m_u}, hf^u_{m_u})$.
5: I send e to u and deduct an amount of v from u's account.
6: End

In some scheme, such as [11, 13], CREATE process is not an independent process. It exist as a part of SETUP process. In this scheme, a medium m is a part of user u's system parameter a_u. The electronic cash data e can be used multiple times, with each usage has a value of fixed v. With these conditions, this scheme still fulfill Definition 1 and Definition 10.

3.3 SPEND Process

This part of the model describes the core process of electronic cash system, which is the exchange of e. This process only involves a user u and a merchant r. The definition of this model is as follows.

Definition 11. *For a pair of user $u \in U$ and a receiver $r \in R$,* SPEND(u, r, e) *is an operation to exchange electronic cash data e from u to r by using Algorithm 3.*

Algorithm 3 SPEND Algorithm

1: Begin
2: u and r agree on a value v.
3: u send $e = f(vf^v_m, hf^u_m)$ to r.
4: **if** r verify that $f(m, v) = vf^v_m$ AND $f(m, u) = hf^u_m$ AND $vf^v_m \geq v$ **then**
5: r create a receipt $r_t = f(u, r, e, a_r)$.
6: **else**
7: r reject and abort process.
8: **end if**
9: End

Some scheme may delegate the verification process in Algorithm 3 to I. In this scheme, r simply contact I and send the transaction data (e, u, r, a_r) to I (this step usually found at on-line scheme). Since in the end r still receive the result of verification and decide to continue or not, the process still fulfill Definition 11.

3.4 DEPOSIT Process

An electronic cash data life cycle when it is returned to I. DEPOSIT process explains the steps to terminate an electronic cash data usage. This process can be considered as a process to change electronic cash to cash, or an opposite process of CREATE. The definition of this process is as follows.

Definition 12. *For each e received by a $r \in R$,* DEPOSIT *is an operation between r and I to settle the usage of e by using Algorithm 4.*

Algorithm 4 DEPOSIT Algorithm

1: Begin
2: r send I a set of electronic cash data $e_1, e_2, \ldots, e_n$, where n is the number of electronic cash data to be settled.
3: **for all** e in set **do**
4: **if** I verify $vf^v_m = f(v)$ AND $vf^v_m \notin L_e$, where L_e is a list of used e **then**
5: I add v to r account.
6: I add e_n to list L_e so that $L_e \cup e_n$.
7: **else**
8: I reject e_n.
9: **end if**
10: **end for**
11: End

I may find a data that has been used before or formed without proper protocol. After finding such data, I can use ARBITRATE process to track the responsible user.

3.5 ARBITRATE Process

Some dispute may arise from the usage of electronic cash. A user may forges a data and uses it on a transaction. A merchant may receives a double spent electronic cash. A dishonest issuer may accuses honest user of doing double spend. To settle these disputes, we need to prove two things. First we need to validate the electronic cash data, by proving the value function and holder function. Second is to determine the adversary identity.

ARBITRATE models the process to determine the validity of e or to identify of an adversary. The model is defined as follows.

Definition 13. *For a dispute between any entity $i \in E \rightarrow i \neq P$ over a transaction of e,* ARBITRATE *is an operation conducted by P to determine the usage of e or to trace any entity involved with e by using Algorithm 5.*

Algorithm 5 ARBITRATE Process

Begin
An entity i request an arbitration to P.
i send data of the disputed transaction (e, r_t).
if P verify $f(m, v) = vf_m^v$ AND $vf_m^v \notin L_e$ **then**
  e is valid.
else
  e is forged or double spent.
end if
if P verify $r_t = f(u, r, e)$ **then**
  The transaction between u and r is valid.
else
  The transaction is not valid.
end if
if The user $u \in f(m, u) = hf_m^u$ **then**
  P prove the ownership of u over e.
else
  u is not the owner of e.
end if
End

4 Model of Electronic Cash Properties

We present a list of property model commonly found in electronic cash scheme. The property can be divided into two general categories: functional, and security. It is not mandatory to implement all properties in a scheme. However, two security properties must exist for a scheme to be functional.

4.1 Functional Property

Functional property model covers all property that can help the operation of electronic cash system. This type of property is not mandatory, a scheme can operates appropriately without a functional property. However, some scheme may gains additional benefit by implementing this property. The model of electronic cash functional property consist of *divisibility, peer-to-peer*, and *transferable*.

Divisibility describes the behavior of electronic cash data value function. A divisible electronic cash data can be used multiple time by an user without changing its medium. The value function of electronic cash with this property can be divided into smaller value. We define divisibility as follow:

Definition 14. *Divisible electronic cash is a system of $\hat{e}$ where for each e, the value function for a certain medium vf_m^v is a sum of arbitrary smaller values v_n. Each v_n can be used in any n transaction by the same $u \in U$. The value function of divisible electronic cash must satisfy:*

$$vf_m^v = vf_m^{v_1} + vf_m^{v_2} + \ldots + vf_m^{v_n},$$

where

$$v = v_1 + v_2 + \ldots + v_n.$$

Definition 14 also complies to Definition 8. This means that divisible electronic cash has the form of variable-valued electronic cash. It is also means that variable-valued type of e-cash always has the divisible property.

Peer-to-peer is a property that describes the implementation behavior of SPEND process. As we have stated before, the verification of e can be delegated to I. If a scheme can use SPEND without involving any entity beside r and u, the scheme has the property of peer-to-peer. The complete definition is as follows.

Definition 15. *A system $\hat{e}$ is a peer-to-peer electronic cash system if for any* SPEND *process there is an ordered pair with an exact member, such as* $\{(U, \texttt{SPEND}), (R, \texttt{SPEND})\}$.

By Definition 11, an user u transfers electronic cash to r without changing its holder function. This electronic cash data cannot be used in another transaction by r and it must be settled by using DEPOSIT process. Transferable property alter this behavior, it enables the transfer of electronic cash data ownership by alters its holder function. The receiver can used the electronic cash data in another transaction. The definition of this property is as follows.

Definition 16. *A system $\hat{e}$ is having a transferable property if for all e there can there is a* SPEND *process between two user, u_1, u_2 and $u_1 \neq u_2$, so that the process fulfill:*

$$f(vf_{m_t}^{v_t}, hf_{m_t}^{u_2}) = f(vf_{m_2}^{v_2}, hf_{m_2}^{v_2}) + f(vf_{m_1}^{v_1}, hf_{m_1}^{u_1}),$$

where t denotes the time after SPEND *process,*

$$\begin{aligned} v_t &= v_2 + v_1, \\ m_t &= m_2 + m_1. \end{aligned}$$

Transferable property simplify the entity set E. In a system with transferable property, it is applies that $U = R$. There is no need to set up the parameter of different group of entity thus reducing the system complexity. The example of scheme with this property can be found in [1].

4.2 Mandatory Security Property

Within any monetary system, forgery poses significant threat to the entire system. In electronic cash system, a user who able to forge electronic cash data can generate any number of data without the proper process. As a result, the system cannot be trusted for further operation. Therefore, the property of unforgeability is a must. We define unforgeabiltity as follows.

Definition 17. *A system $\hat{e}$ is said to have unforgeability if $\forall u, r \in E$ there is no non-negligible advantage to form a valid e without using* CREATE *process.*

Double spending is an action where a user, or a receiver, uses a value function more than once in a different transaction (SPEND process). This action is a variation of forgery. However, if in forgery the value function and

holder function is not valid data, in double spend both value is a valid data made by a proper process.

A system of $\hat{e}$ must have a mechanism to detect double spent data to prevent (or to search for the perpetrator) double spending. For example, using the list L_e from Algorithm 4, an entity can determine whether a data has been used before or not. To model this property in more formal manner, we define the property of double spending prevention as follows.

Definition 18. *A system $\hat{e}$ is said to have double spending prevention property if $\forall u \in U$ there is no non-negligible advantage to execute two or more* `SPEND` *process to any $r_1, r_2 \in R$ with the same $e = f(vf_m^v, hf_m^u)$. Or, $\forall r \in R$ there is no non-negligible advantage to execute two or more* `DEPOSIT` *process for a single $e = f(vf_m^v, hf_m^u), \forall u \in U$.*

The advantage described in Definition 17 and Definition 18 not only refers to the probability of success of forgery or double spending. The phrase also refers to the feasibility of the actions. If a scheme has non-negligible probability but infeasible to do the forgery or double spending, the adversary is considered to have negligible advantage to do the action.

4.3 Optional Security Property

The optional security properties are not mandatory, such as unforgeability and double spending prevention. The electronic cash system still secure in the absence of these properties. However, the implementation of these properties will add additional layer of security into the scheme.

The first property is *anonymity*. The works of Cannard-Gouget classify anonymity into 4 different levels: weak, strong, full, and perfect anonymity [2]. However, the notion of anonymity of Cannard-Gouget classification merges anonymity with *unlinkability*. To prevent the confusion between the two notions, we models anonymity with unlinkability separately. The fulfillment of Cannard-Gouget classification in this model, depends on the fulfillment of anonymity and unlinkabiltiy in this paper. In this paper, we define anonymity as follows.

Definition 19. *Let $r_t(e)$ be a transaction receipt of a certain* `SPEND` *process between $u \in U$ and $r \in R$. A system $\hat{e}$ has the property of anonymity if for any entity $i \in E, i \neq \{u, r, P\}$, there is no non-negligible advantage to determine that $\{u, r\} \in r_t(e)$.*

Unlinkability is a property that ensure that no one can track the movement of electronic cash data. If an adversary can see two distinct transactions, he/she shall not be able to link the two transaction to a user (even if both transaction involve the same user). We define the unlinkability as follow:

Definition 20. *Let e_1, e_2 be two distinct electronic cash data owned by $u \in U$, and r_1, r_2 be the transaction receipt of e_1, e_2 respectively. A system $\hat{e}$ has the unlinkability property if for any entity $i \in E, i \neq \{u, P\}$, there is no non-negligible advantage to determine that:*

$$\{u\} \in r_1(e_1) \cap r_2(e_2),$$

where

$$\begin{aligned} e_1 &= f(hf_{m_1}^u), \\ e_2 &= f(hf_{m_2}^u). \end{aligned}$$

The last security property related to the common assumption in electronic cash scheme. Many scheme assume that entity I is trusted by the entire system. It is assumed that I will not deliberately conduct any action that disadvantageous to another honest entity.

The *exculpability* property disregards this assumption of I. A scheme that has exculpabilty property (such as [25]) deploys a mechanism to ensure that I can be trusted. The exculpability property prevent I to accuse an honest user of double spending. It also prevent I to create e without any request from u. We define exculpability as follows.

Definition 21. *A system $\hat{e}$ have exculpability property if for any honest user $u \in U$ and a non-exist electronic cash data e_x, there is no non-negligible advantage for I to claim that $e_x \in L_e \leftrightarrow$* `SPEND`*$(u, r, e_x)$ or that $e_x = f(hf_m^u)$.*

5 Using The Model for Security Analysis

At this section, we will use our model to analyze the security of an existing electronic cash scheme. We use this activity to validate our model. We aim to analyze the security of Chaum's Untraceable Electronic Cash scheme [6] using our model.

As a starting point, we define the electronic cash data e in this scheme (from this point, we will refer Chaum's scheme as "scheme"), which in form of

$$C = \prod_{1 \leq i \leq k/2} f(x_i, y_i)^{1/3} mod\ n. \tag{2}$$

The identity of a user is represented by an account number u and a counter v. Both values are components of $y_i = g(a_i \oplus (u||(v+i)))$. Each C has a fixed denomination of v. These conditions fulfill Definition 1 and Equation (1) to describe e. It can also be noted that the scheme fulfill Definition 7, which make it a fix-valued electronic cash.

The electronic cash data in the scheme is made by using withdraw protocol between a user and the bank (issuer of electronic cash data, hence I). The steps of this process can be summarized as follows.

From Algorithm 6, we can see that all the variables needed to construct C is made by the user. The bank only verify the ownership of B_i and debit the user account. There is no process that involve the bank secret parameter in the construction of C. With this condition,

Algorithm 6 Withdraw Process of [6]

1: Begin
2: The user choose a_i, c_i, d_i and r_i, where $1 \leq i \leq k$, randomly from residue of *mod* n.
3: The user send $B_i = r_i^3.f(x_i, y_i) mod\ n$, for all i, where $x_i = g(a_i, c_i)$ and $y_i = g(a_i \oplus (u||(v+i)))$ to bank.
4: The bank choose $R = \{i_j\}$, where $1 \leq i_j \leq k, 1 \leq j \leq k/2$.
5: **for all** $i \in R$ **do**
6: The user send a_i, r_i, c_i, d_i to the bank.
7: **end for**
8: The bank send the user $\prod_{i \notin R} B_i^{1/3} = \prod_{1 \leq i \leq k/2} B_i^{1/3} mod\ n$.
9: The user extract the electronic cash data $C = \prod_{1 \leq i \leq k/2} f(x_i, y_i)^{1/3} mod\ n$.
10: End

the user actually can produce C without using the withdraw protocol with great probability. The user only needs to choose a set of a_i, c_i, d_i, and r_i and construct C using step 9 in Algorithm 6. Therefore, the scheme is not fulfilling Definition 17.

The scheme need to fulfill the second mandatory property of security, the double spending prevention. The double spending prevention mechanism could be analyzed from the scheme's `SPEND` and `DEPOSIT` action. In the scheme, both action are combined into one protocol. The protocol is summarized in Algorithm 7.

Algorithm 7 Spend Protocol of [6]

1: Begin
2: The user u send C to the receiver r.
3: r choose a binary string, $z_1, z_2, \ldots, z_{k/2}$ and send it to u.
4: **for all** z_i in binary string **do**
5: **if** $z_i = 0$ **then**
6: u send $x_i, a_1 \oplus (u||(v+i))$ to r.
7: **else**
8: u send a_i, c_i, y_i to r.
9: **end if**
10: **end for**
11: **if** r can verify the correctness of C **then**
12: r accept C.
13: **else**
14: r reject C.
15: **end if**
16: r send C, the binary string $(z_1, z_2, \ldots, z_{k/2})$, and all u's responses to I.
17: **if** I can verify the transaction **then**
18: I credit r account.
19: **else**
20: I reject the transaction.
21: **end if**
22: End

Step 16 to 21 in Algorithm 7 can be executed separately from the rest of steps. These steps represent the `DEPOSIT` action in the scheme. The receiver may wait until end of the day to execute theses steps for all transaction he/she receives in the day. This delay may result in a double spending attempt by the user.

According to Algorithm 7, the receiver cannot check whether a data has been used before by the same user. Therefore, it is quite possible for a user to spend a data in a receiver, then uses the same data in another transaction with another receiver. However, using step 16 to 21, I can detect the double spender quite easily and run a tracing algorithm to determine the user identity. If a user double spend an electronic cash data, then I will, with great probability, acquires both a_i and $a_i \oplus (u||(v+i))$ components of the same i in the electronic cash data. By using XOR operation on both components, I can extract $(u||(v+i))$ which contains the user's identity u. In short, it is quite improbable for an u to conduct a double spend without being detected and traced by I. Thus, the scheme fulfill Definition 18.

From Algorithm 7, we can also see that the `SPEND` process involves two entities: the user and the receiver. The receiver validates the electronic cash data without the help of another entity. This condition fulfill the description in Definition 15, which make the scheme has the property of *peer-to-peer*.

6 Comparison with Another Model

As we have stated earlier, we build our model based on the model of Inenaga *et al.* [15]. We find that the model in Inenaga *et al.* only covers a portion of electronic cash system. The model can only be used to describe an off-line electronic cash (peer-to-peer) involving only two entities. The complete comparison between our model and Inenaga *et al.* model can be seen in Table 1.

The model proposed by Inenaga *et al.* cannot be used to model scheme such as find in Kang & Xu [16], even when the scheme uses off-line transaction. The Kang & Xu scheme involve entity such as Bank and Trustee, which is not described in Inenaga *et al.* model. The scheme of Kang & Xu is built with property of anonymity as its goals, which is not found in the model of Inenaga et al. At best, the model of Inenaga *et al.* can only models small part of Kang & Xu's scheme.

On the contrary, Bank and Trustee is covered in our model as Issuer and Principal. Our model also provide a property model that can explain anonymity. Compared to Inenaga *et al.* model, our model can easily models the entire scheme of Kang & Xu. This illustrate our model's capability to model a wider range of electronic cash scheme compared to Inenaga *et al.* model.

Table 1: Comparison of models

Model	SubModel of System	SubModel of Process	SubModel of Property
Inenaga *et al.*	Money System E-money Type	Money Transfer	Money Forgery Forged Money Transfer Detectability of Forged Money
Proposed	Electronic cash data Electronic cash system Electronic cash form	SETUP CREATE SPEND DEPOSIT ARBITRATE	Functional Property Security Property

7 Conclusions

The proposed model has more comprehensive approach compared to the model in [15]. Figure 2 shows the resume of our model. We divide the model into 3 sub models: the model of system, the model process, and the model of properties. Due to its generality, our model can be used to describe most of existing electronic cash scheme. However, it cannot be used to describe a specific mechanics used in specific scheme. For example, the model of `SPEND` process cannot describe the process of updating electronic cash record to the entire system in scheme [25].

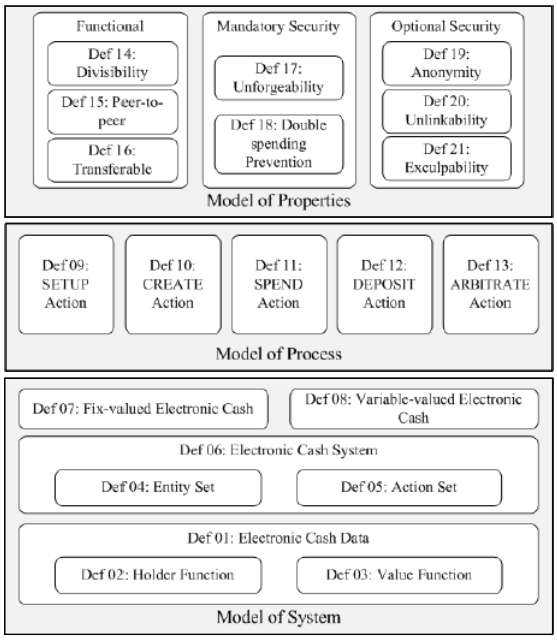

Figure 2: The proposed model

The proposed model can be used as a helping tool to build new electronic cash scheme. The model can be considered as a skeleton to build more detailed scheme. Any person can use the model as a reference on how electronic cash should behave. By using the security property model, the builder of the scheme can ensure that their scheme has the proper security mechanism.

As we have shown in previous example, our model is suited as a reference to compare or evaluate existing scheme. By using our model, any method of evaluation, such as in [7, 9, 28], can have a clear definition on determining the performance of the evaluated scheme. By having a clear definition of security objective, we can avoid mistakes because of the difference in security definition.

We also believe that our model can be used to help the development of payment scheme on a specific platform but not necessarily electronic cash scheme, such as scheme in [10, 12, 17, 24]. Although, the two scheme does not explicitely uses electronic cash, it has the same fundamental principle. The electronic cash and these payment schemes have more similarity compared to electronic cash and cryptocurrency.

This model does not cover distributed electronic cash or cryptocurrency, such as Bitcoin, due to the difference in underlying mechanism. However, we find that the basic principle of centralized and distributed electronic cash is the same. For example, both centralized and distributed electronic cash must have unforgeability and double spending prevention property. It is interesting to expand this model to cover distributed electronic cash

There are many attempt to use centralized electronic cash scheme as a mixing agent to increase the anonymity property of distributed electronic cash scheme. Scheme such as [8, 14, 20, 21, 27], using centralized electronic cash mechanism to create a masking medium to Bitcoin. These schemes has more similarity to centralized electronic scheme while operating under the paradigm of distributed electronic cash. These schemes is suitable as the first stepping stone to develop more general model that covers distributed electronic cash.

References

[1] O. Blazy, S. Canard, G. Fuchsbauer, A. Gouget, H. Sibert, and J. Traoré, "Achieving optimal anonymity in transferable e-cash with a judge," in *International Conference on Cryptology in Africa*, pp. 206–223, 2011.

[2] S. Canard and A. Gouget, "Anonymity in transferable e-cash," in *International Conference on Applied Cryptography and Network Security*, pp. 207–223, 2008.

[3] S. Canard, A. Gouget, and J. Traoré, "Improvement of efficiency in (unconditional) anonymous transferable e-cash," in *International Conference on Financial Cryptography and Data Security*, pp. 202–214, 2008.

[4] S. Canard, D. Pointcheval, O. Sanders, and J. Traoré, "Divisible e-cash made practical," *IET Information Security*, vol. 10, no. 6, pp. 332–347, 2016.

[5] D. Chaum, "Blind signatures for untraceable payments," in *Advances in cryptology*, pp. 199–203, 1983.

[6] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in *Conference on the Theory and Application of Cryptography*, pp. 319–327, 1988.

[7] Y. Chen and J. S. Chou, "On the privacy of user efficient recoverable off-line e-cash scheme with fast anonymity revoking," *International Journal Network Security*, vol. 17, no. 6, pp. 708–711, 2015.

[8] G. Danezis, C. Fournet, M. Kohlweiss, and B. Parno, "Pinocchio coin: Building zerocoin from a succinct pairing-based proof system," in *Proceedings of the First ACM workshop on Language Support for Privacy-enhancing Technologies*, pp. 27–30, 2013.

[9] J. Dreier, A. Kassem, and P. Lafourcade, "Formal analysis of e-cash protocols," in *12th International Joint Conference on e-Business and Telecommunications (ICETE'15)*, vol. 4, pp. 65–75, 2015.

[10] T. H. Feng, M. S. Hwang, and L. W. Syu, "An authentication protocol for lightweight NFC mobile sensors payment," *Informatica*, vol. 27, no. 4, pp. 723–732, 2016.

[11] M. S. Hwang, C. C. Lee, Y. C. Lai, "Traceability on low-computation partially blind signatures for electronic cash", *IEICE Fundamentals on Electronics, Communications and Computer Sciences*, vol. E85-A, no. 5, pp. 1181–1182, May 2002.

[12] M. S. Hwang, I. C. Lin, L. H. Li, "A simple micropayment scheme", *Journal of Systems and Software*, vol. 55, no. 3, pp. 221–229, Jan. 2001.

[13] M. S. Hwang and P. C. Sung, "A study of micropayment based on one-way hash chain," *International Journal Network Security*, vol. 2, no. 2, pp. 81–90, 2006.

[14] M. H. Ibrahim, "Securecoin: A robust secure and efficient protocol for anonymous bitcoin ecosystem," *International Journal Network Security*, vol. 19, no. 2, pp. 295–312, 2017.

[15] S. Inenaga, K. Oyama, and H. Yasuura, "Towards modeling stored-value electronic money systems," *Information and Media Technologies*, vol. 6, no. 1, pp. 25–34, 2011.

[16] B. Kang and D. Xu, "Secure electronic cash scheme with anonymity revocation," *Mobile Information Systems*, vol. 2016, 2016.

[17] I. C. Lin, M. S. Hwang, C. C. Chang, "The general pay-word: A micro-payment scheme based on n-dimension one-way hash chain", *Designs, Codes and Cryptography*, vol. 36, no. 1, pp. 53–67, July 2005.

[18] J. Liu and Y. Hu, "A new off-line electronic cash scheme for bank delegation," in *5th International Conference on Information Science and Technology (ICIST'15)*, pp. 186–191, 2015.

[19] J. W. Lo, H. M. Lu, T. H. Sun, and M. S.Hwang, "Improved on date attachable electronic cash," *Applied Mechanics and Materials*, vol. 284, pp. 3444–3448, 2013.

[20] I. Miers, C. Garman, M. Green, and A.D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *IEEE Symposium on Security and Privacy (SP'13)*, pp. 397–411, 2013.

[21] K. Naganuma, M. Yoshino, H. Sato, and T. Suzuki, "Auditable zerocoin," in *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW'17)*, pp. 59–63, 2017.

[22] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Bitcoin*, 2008. (`https://bitcoin.org/en/bitcoin-paper`)

[23] H. Oros and C. Popescu, "A secure and efficient off-line electronic payment system forwireless networks," *International Journal of Computers Communications & Control*, vol. 5, no. 4, pp. 551–557, 2010.

[24] H. H. Ou, M. H. Hwang, and J. K. Jan, "A provable billing protocol on the current umts," *Wireless Personal Communications*, vol. 55, no. 4, pp. 551–566, 2010.

[25] T. Sander and A. Ta-Shma, "Auditable, anonymous electronic cash," in *Annual International Cryptology Conference*, pp. 555–572, 1999.

[26] D. E. Saputra and S. H. Supangkat, "A study of electronic cash paradigm," in *International Conference on Information Technology Systems and Innovation (ICITSI'14)*, pp. 273–278, 2014.

[27] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *IEEE Symposium on Security and Privacy (SP'14)*, pp. 459–474, 2014.

[28] F. Wang, C. C. Chang, and C. Lin, "Security analysis on secure untraceable off-line electronic cash system.," *International Journal Network Security*, vol. 18, no. 3, pp. 454–458, 2016.

Biography

Dany Eka Saputra received B.Eng. in Aeronautics and Astronautics from Institut Teknologi Bandung in 2007. He also obtained his M.Eng. in Electrical Engineering from the same university in 2012. Currently, he is taking his Doctoral Study in Electrical Engineering and Informatics from Institut Teknologi Bandung. He also a faculty member of Departement of Informatics at STMIK "AMIKBANDUNG". His main interest is information security with specialization in electrical cash security. His other interests include game tecnology and protocol

engineering.

Sarwono Sutikno received B.Eng. in Electronics from Institut Teknologi Bandung in 1984. He then received his Dr.Eng. in Integrated System from Tokyo Institute of Technology in 1994. Currently, he is an Associate Professor at Institut Teknologi Bandung. An active member of ISACA with several certification. His main interests are information security and cyber security.

Suhono harso Supangkat received his B.Eng. in Electrical Engineering from Institut Teknologi Bandung in 1986. He received his Dr.Eng. in Information System Science from Tokyo University of Electro-communication in 1998. Currently, he is a Professor at Institut Teknologi Bandung. His main interest is smart city system and technology. Actively promoting smart city concept and technology from 2012.