IMES DISCUSSION PAPER SERIES

A Technical Examination of Non-Ledger-Based Payment Systems

Yuko Tamura, Masayuki Abe, Tetsuya Okuda,
Hiromasa Tsugawa, Toshiyuki Miyazawa, Kazuki Yamamura,
Yoshiharu Akahane, Tomoki Taguchi, Yuto Hirakuri,
Hiroto Masuda, and Kento Yamada

Discussion Paper No. 2025-E-7

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

2-1-1 NIHONBASHI-HONGOKUCHO

CHUO-KU, TOKYO 103-8660

JAPAN

You can download this and other papers at the IMES Web site:

https://www.imes.boj.or.jp

IMES Discussion Paper Series 2025-E-7

August 2025

A Technical Examination of Non-Ledger-Based Payment Systems

Yuko Tamura*[1], Masayuki Abe*[2], Tetsuya Okuda*[2], Hiromasa Tsugawa*[2], Toshiyuki Miyazawa*[2], Kazuki Yamamura*[2], Yoshiharu Akahane*[3], Tomoki Taguchi*[3], Yuto Hirakuri*[3], Hiroto Masuda*[3], and Kento Yamada*[3]

Abstract

This paper explores a payment system that enables transactions without relying on a ledger or intermediary service providers, examining it from a technical perspective. The system facilitates payments through the transmission and receipt of electronic data, analogous to physical cash. In the field of cryptography, this concept has been studied under the name "electronic cash." While several demonstration experiments were conducted in the 1990s, it is presumed that the technology at the time could not ensure sufficient usability. In this paper, we revisit the concept of electronic cash in light of technological advancements and evolving societal needs. Additionally, we conduct practical verification using smartphones to demonstrate that current technological standards can offer electronic cash systems with high usability. From a technical standpoint, we propose methods to further enhance usability and privacy for electronic cash schemes. These include mechanisms for splitting and aggregating electronic cash into arbitrary amounts, as well as schemes that make it difficult to link electronic cash transactions made by the same user. It should be noted that this paper focuses solely on the technical aspects of electronic cash and does not examine the feasibility of its legal, institutional, or practical implementation in society.

Keywords: digital payments; electronic cash; e-money; privacy protection; smartphone payments

JEL classification: L86, L96

*[1] Institute for Monetary and Economic Studies, Bank of Japan (E-mail: yuuko.tamura@boj.or.jp)

*[2] Social Informatics Laboratories, NTT Corporation (E-mail: msyk.abe@ntt.com)
(Miyazawa is currently in Service Innovation Laboratory Group, NTT Corporation)

*[3] Third Financial Sector, NTT DATA Corporation (E-mail: yoshiharu.akahane@nttdata.com)

The authors would like to thank Professor Atsushi Fujioka (Kanagawa University) and Professor Noboru Kunihiro (University of Tsukuba). The views expressed in this paper are those of the authors and do not necessarily reflect the official views of the Bank of Japan, NTT Corporation, and NTT DATA Corporation.

Contents

1. Introduction

Most of the cashless payment systems currently in widespread use adopt a "ledger-based" approach. Here, a ledger refers to a database that records transaction details based on instructions from users, consolidating and managing all transactions and balances for all users. A typical example is deposit transactions, and it appears that recently popularized QR code-based payments also use this approach. Cryptographic assets[1], although differing in the entity and method of ledger management, can also be cited as an example of a ledger-based system. In these ledger-based systems, users issue payment instructions to service providers (or blockchain nodes in the case of cryptographic assets) via the Internet, and the service providers execute the payment by updating the ledger.

In contrast, "electronic cash"[2] (Okamoto and Ohta [1993], Nakayama *et al*. [1997]) enables payments without relying on a ledger, representing a significant departure from existing cashless payment systems. Electronic cash facilitates payments through the transmission of electronic data that functions as physical cash. Payments can be made via data communication between the sender and recipient, resembling the exchange of physical cash. This approach, therefore, potentially offers advantages over ledger-based systems in terms of server fault tolerance, network failure resilience, transaction processing performance, and interoperability with external systems. Furthermore, as the payment process is confined to the two parties involved, transaction details can be kept confidential from service providers. Additionally, when using short-range communication between devices, payments can be made in environments disconnected from the Internet.

The feasibility of electronic cash has been examined in several pilot experiments[3]. For instance, the "Internet Cash" experiment conducted in 1998 tested a system where Internet Cash (electronic cash) issued online was stored on IC cards and could be sent to online stores or

[1] Before the amendment of the Payment Services Act that came into effect in May 2020, this was called "virtual currency."

[2] Nakayama *et al*. [1997] referred to the proposed payment method as "electronic money." In recent years, contactless IC cards are often referred to as "electronic money." Therefore, this paper uses the term "electronic cash," which Okamoto and Ohta [1993] used. The "electronic cash" discussed in this paper is different from the Central Bank Digital Currency (CBDC) being studied by the government and the Bank of Japan.

[3] Demonstration experiments based on the electronic cash system include experiments conducted in December 1995 (NTT Corporation [1995]), September 1996 (NTT Corporation [1996]), September 1998 to February 2000 (Cyber Business Council [2000]), and April 1999 to May 2000 (NTT Communications Corporation [2000]).

friends. However, ensuring sufficient usability[4] with the technology available at the time proved difficult, and electronic cash did not gain traction. Subsequently, the spread of contactless IC-card-based e-money led to a temporary halt in the study of electronic cash.

Recently, the promotion of cashless payments by the government has led to a year-on-year increase in the use of various cashless payment services, including e-money. In 2023, the cashless payment ratio in Japan rose to approximately 40% (Ministry of Economy, Trade and Industry [2024]). The government has set a final target of 80% for the cashless payment ratio (Consumer Affairs, Distribution and Retail Industry Division, Commerce and Service Group, Ministry of Economy, Trade and Industry (METI) [2018]), suggesting that the use of cashless payment services will continue to grow. This anticipated growth underscores the importance of considering the potential impact of server failures and network disruptions on domestic payment services. In this context, exploring non-ledger-based payment systems could contribute to achieving a stable cashless society.

Against this backdrop, this paper first revisits the concept of electronic cash in light of recent technological advancements and societal needs. It then reports on practical verification using commonly available smartphones to evaluate usability under current technological standards. Furthermore, the paper explores methods to enhance the usability of electronic cash schemes and proposes approaches to strengthen user privacy. It is important to note that this study focuses solely on the technical aspects of electronic cash and does not address legal, institutional, or operational feasibility for societal implementation.

The structure of this paper is as follows: Chapter 2 organizes the basic framework of electronic cash systems and the properties required of electronic cash, while discussing the balance between privacy protection and transparency. Chapter 3 reviews the results of practical tests on the transmission and receipt of electronic cash items and evaluates its usability under current technological standards. Chapter 4 explores efficiency improvements in electronic cash systems, including methods to optimize transmission, receipt, and redemption, as well as approaches to enable the splitting and aggregation of electronic cash items and enhance privacy. Finally, Chapter 5 concludes with future prospects and closes the paper.

[4] Usability refers to the ease of use for users. It is similar to “convenience,” and in this paper, it refers to one of the properties required of electronic cash system (safety, convenience, inheritance of benefits of physical cash, and transparency) defined in Chapter 2 (2).

2. Basic framework of the electronic cash system

(1) Differences between the ledger-based system and the electronic cash system

Most payment services currently available use a ledger-based system, where a service provider intermediates the transactions. The service provider records the transaction details in the ledger after receiving a remittance instruction from the user. For example, in the case of deposit transactions, financial institutions execute the transfer by deducting from the sender's account balance and adding to the receiving user's account balance as recorded in the ledger (refer to Figure 1).

On the other hand, methods allowing payment without a ledger have also been considered in the past (Okamoto and Ohta [1993], Nakayama *et al.* [1997]). These aim to enable payment by transmitting electronic data directly from the sender to the recipient, similar to physical cash, and are referred to as "electronic cash." Electronic cash items are stored on user devices such as smartphones[5], and the transfer can occur via the Internet or through proximity-based wireless communication technologies in face-to-face scenarios (refer to Figure 1).

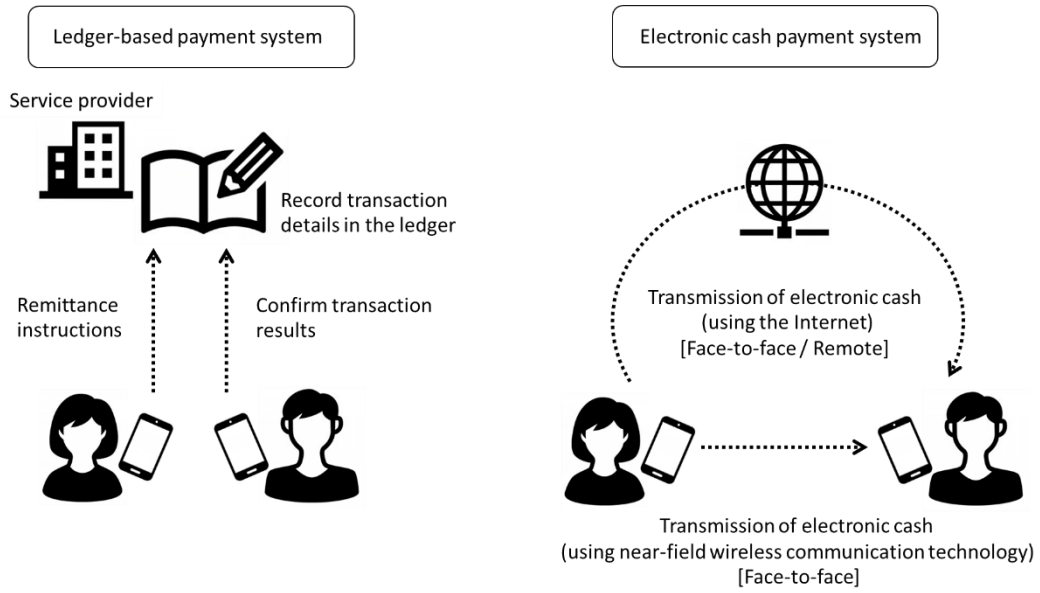


Figure 1: Comparison of ledger-based payment system and electronic cash payment system

[5] Although this paper assumes a smartphone as the device used by the user, the electronic cash system can be implemented on a computer equipped with a tamper-resistant device similar to embedded Secure Element (eSE). SE is a module that is highly secure against external attacks and is implemented by combining hardware and software. The type built into the smartphone is called eSE. Tamper resistance refers to resistance to unauthorized reading and alteration of internal information. The necessity of tamper resistance is summarized in section (4) of this chapter.

Electronic cash system, therefore, enables payments without involving a service provider. While the provider's involvement is necessary for user registration and issuance of electronic cash items, the transmission process can be confined to data communication between the sender and the recipient. Consequently, electronic cash system offers the following advantages: resilience to server disruptions (less affected by server outages); resilience to network disruptions (possibility of making payments without Internet access); high processing efficiency (dependent on the device's processing power rather than the provider's servers or network bandwidth); and privacy of transaction details from the provider (the provider does not have real-time visibility into transactions).

Additionally, the electronic cash system can easily integrate multiple services. For instance, combining electronic cash items issued by different providers or exchanging different electronic cash types requires the providers to connect their ledgers via Application Programming Interfaces (APIs) in a ledger-based system. However, in an electronic cash system, the absence of ledgers eliminates the need for such inter-provider API connections. Users can simply install the necessary applications on their devices to facilitate service integration.

In addition, taking advantage of the feature that allows the modification of service formats through applications on the user side without requiring system updates on the service provider's side, it is possible to introduce programmability[6] to electronic cash. Here, "programmability" refers to the ability for entities other than the service provider to apply unique rules for using electronic cash. Users within the applicable scope can program these unique rules into their devices to execute them individually. Furthermore, by embedding usage rules for electronic cash items at the time of issuance, the service provider may provide programmable money[7]. For example, rules such as imposing expiration dates on electronic cash items or restricting the scope of its usage could be implemented.

On the other hand, one concern regarding the electronic cash system is the implications of storing electronic cash items solely on the user's device. In ledger-based systems, all asset data

[6] Programmability in payment systems means that various entities, not only operators of payment systems, can program settlement functions according to their individual needs (Hojo and Hatogai [2022]).

[7] Programmable money is a concept that focuses on controlling individual behavior by storing attribute information and programs specific to "objects" called fund data (Hojo and Hatogai [2022]). Since electronic cash is issued as a digital signature of the service provider to the serial number (see BOX 1 of section (3) of this chapter), it is possible to write rules on the use of electronic cash in the message part of the signature.

are managed by the service provider. Therefore, even if a user loses their device, as long as their identity can be verified, access to their data could theoretically be restored. In contrast, with the electronic cash system, since the electronic cash items are stored within the user's device, losing the device means losing the electronic cash items as well[8]. This characteristic is similar to physical cash. Additionally, attention must be paid to the requirement that user devices possess a certain level of tamper resistance[9] (see section (4) of this chapter).

This paper assumes that the medium for storing electronic cash items is a user-owned device, such as a smartphone. However, in the future, it may become possible to store electronic cash items in secure areas outside of the device. For example, in discussions surrounding the advancement of networks for the sixth-generation mobile communication system (6G)[10], there is consideration of equipping mobile networks with advanced encryption and secure computation functions to robustly protect user information. The Trusted Execution Environment (TEE)[11] is also included in this scope (as reported by the Network Service Systems Laboratory of NTT Corporation, 2023). When such advancements in network security are realized, it may be possible to address the risk of device loss by storing the device owner's electronic cash items within the TEE environment at the edge of the network (e.g., base stations that serve as mobile network entry points) linked to the user's device.

(2) Properties required of the electronic cash system

Nakayama *et al*. [1997] outlined the desired properties of electronic cash: safety, convenience, and the preservation of the inherent advantages of physical cash. From the need to consider measures for anti-money laundering and countering the financing of terrorism (AML/CFT) in

[8] The service provider may back up all electronic cash items in preparation for the loss of the device, but in that case, it will be necessary to send and maintain backup data, so it will have the same risk of failure as the ledger-based systems.

[9] Specifically, this is achieved by protecting data by leaving traces of intrusion or erasing data against unauthorized access. Specific functions include tamper evidence, which provides evidence of unauthorized access; tamper resistance, which protects data from unauthorized access; and tamper response, which erases data against unauthorized access (Tamura and Une [2007]).

[10] With the advancement of mobile communication systems that support mobile devices, discussions are underway to deploy not only data transfer but also various information processing functions at the edge (base stations, etc.), which is the entry point to mobile networks. Devices will distribute functionality to the edge and access services over the Internet via mobile networks.

[11] TEE is a function that provides an execution environment for processing that requires high security. This execution environment (TEE space) is separated from the space where normal applications run (Rich Execution Environment (REE)), and communication between the two spaces is designed to be executed under strict access control.

providing payment systems, this paper adds transaction transparency as another essential property of electronic cash.

Safety

(1) Electronic cash should be resistant to forgery, tampering, duplication, and double spending.

Like physical cash, electronic cash must be secure against forgery and tampering. Additionally, due to the replicable nature of electronic data, it must be difficult to duplicate or use twice. From the viewpoint of safety, possible fraudulent actions for electronic cash are as follows.

- Forgery and tampering: Unauthorized creation or modification of electronic cash items
- Duplication usage: Unauthorized copying and usage of another person's electronic cash items
- Double spending: Duplicating and reusing one's electronic cash items

The electronic cash system prevents forgery and tampering through cryptographic techniques like digital signatures. Adding owner-specific information to electronic cash items can prevent unauthorized duplication by a third party. To address double spending, which is harder for payment service providers to detect in real time without a ledger, tamper-resistant devices are employed (see section (4) of this chapter). Additionally, even in cases where the tamper resistance is compromised, the service provider manages the situation by tracking serial numbers, enabling retrospective detection[12].

Convenience

(2) Electronic cash items should allow usage in arbitrary denominations.

(3) It should support both face-to-face and remote payments.

(4) The issuance and management costs of electronic cash items should be low.

Convenience refers to the degree by which electronic cash is easier to use than physical cash for both users and service providers. Users particularly value the ability to divide electronic cash items into arbitrary denominations and the flexibility to use them in both face-to-face and

[12] In the electronic cash system, a database (DB) of serial numbers is required for the retrospective detection of duplication and double spending, but it is different from a ledger for recording settlements.

remote payment scenarios (properties (2) and (3)). For providers, lower issuance and management costs than physical cash (property (4)) are a key benefit.

In the basic scheme introduced in section (3) of this chapter and the verification experiments in Chapter 3, the unit of electronic cash items is fixed, leaving property (2) for future exploration. A method enabling the division and aggregation of electronic cash items is discussed in section (3) of Chapter 4.

Preservation of advantages of physical cash[13]

(5) Difficult to identify past users of electronic cash items (anonymity[14]).

(6) Difficult to link different transactions of the same user (unlinkability).

(7) Capable of offline payments in network-disconnected environments.

(8) Electronic cash items received can be reused for other payments.

(9) Devices required for electronic payments should be portable.

Anonymity, a key feature of physical cash, ensures that recipients cannot deduce past transaction information, even if collusion occurs between merchants and/or financial institutions (Furuichi [1995]). Similarly, electronic cash scheme should protect user privacy, making it difficult to identify past users (property (5)). Additionally, unlinkability is crucial in situations where large amounts of data can be collected and analyzed, ensuring that even with access to multiple electronic cash items' records, it is impossible to correlate them to deduce user activity (property (6)).

Most existing cashless payment methods rely on Internet connectivity. However, offline functionality is essential for scenarios like natural disasters (property (7)), Nakata [2021]). Other usability requirements include the ability to reuse received electronic cash items without returning it to service providers (transferability[15]) and the portability of the payment device to enable settlement anytime and anywhere (properties (8) and (9)).

---

[13] Nakayama *et al*. [1997] also identified the property of supporting multiple financial institutions in addition to properties (5) and (6). Nakayama *et al*. [1997] assumed that electronic cash would be issued against deposits and could be converted back into deposits, suggesting that the ability to deposit it with financial institutions other than the issuing institution would be a desirable feature. However, this paper assumes that electronic cash is issued by payment service providers and does not make the involvement of financial institutions a requirement; therefore, the property of supporting multiple financial institutions is not included.

[14] Nakayama *et al*. [1997] described this as "untraceability" of the user.

[15] A method with this property is called an open-loop type, while a method that does not is called a closed-loop type.

Transparency

(10) Service providers must be able to trace electronic cash items when necessary.

For AML/CFT purposes, payment transparency is essential, enabling the tracing of funds as necessary. This requires service providers to verify users' identity information (name, address, etc.) and ensure its accuracy.

However, excessive user data management could allow providers to identify users based on usage history of redeemed electronic cash items. To balance privacy and transparency, an independent certification authority should handle user authentication[16]. Privacy protection and transparency are further addressed in section (5) of this chapter.

(3) Basic scheme

This section introduces the electronic cash system designed to have the aforementioned properties (Nakayama *et al*. [1997]). The primary entities that make up the electronic cash system are the service provider, the certification authority[17], users (including both senders and receivers of electronic cash items, such as stores), and the users' devices (devices used for sending, receiving, and storing electronic cash items). From here, we describe electronic cash items as electronic cash for brevity. The basic scheme of the electronic cash system consists of the following phases: user registration and certificate issuance[18], electronic cash issuance, electronic cash transmission, electronic cash redemption, and double-spending verification[19] (see Figure 2). The specific flow is described below. For details on cryptographic processing methods, refer to BOX 1.

[16] From the viewpoint of protecting the privacy of users, as in Nakayama *et al*. [1997], it was determined to establish an independent organization to manage user information. However, since this paper does not consider the current legal system, it is necessary to examine the relationship with the legal system separately.

[17] A certification authority verifies the user's identity and issues a certificate for the user's public key. It is possible that multiple service providers may work with a single certification authority.

[18] A certificate issued by a certification authority is used by a third party to verify that the key pair used for cryptographic processing is the correct one registered with the certification authority.

[19] For crypto assets that do not have a specific administrator, there are generally no procedures such as user registration or certificate issuance. Therefore, the user of the crypto asset is not identified, and the key cannot be invalidated even if the key is stolen. However, when using a crypto asset exchange service provider for crypto asset transactions, identity verification by a crypto asset exchange service provider, etc. is required, and since all crypto assets are managed in a ledger, there is no redemption process.

(i) User registration and certificate issuance

When using electronic cash, users generate the key pair necessary for cryptographic processing[20] and obtain a certificate from the certification authority.

(1) The user submits their personal information (e.g., name, address) required for certificate issuance to the certification authority.

(2) The certification authority verifies the user's identity and registers the user's information.

(3) The user generates a key pair consisting of a private key and a public key and sends the public key to the certification authority.

(4) The certification authority associates the public key with the user's information and issues a certificate for the public key to the user.

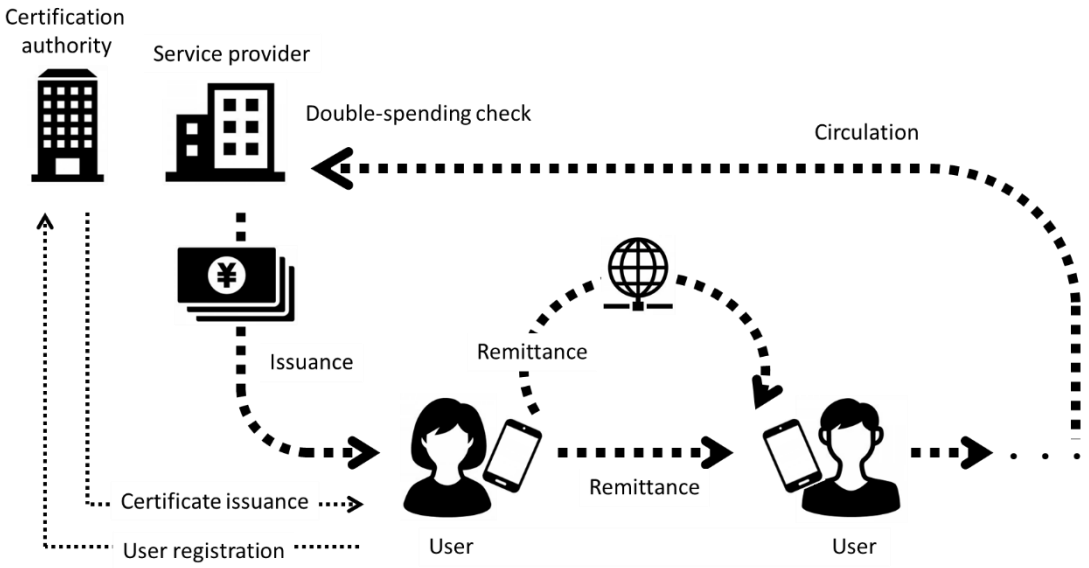


Figure 2: Basic framework of the electronic cash scheme

(ii) Issuance of electronic cash

The service provider issues electronic cash to the user upon request. To prevent forgery and tampering, the electronic cash is digitally signed by the service provider. Additionally, measures are taken against duplication and double spending by designating the owner at the time of

[20] A key pair called a private key and a public key is used for cryptographic processing. The private key must be managed as information known only to the user, while the public key is information that can be disclosed to other users. In the digital signature method, processing using a public key enables confirming that the message to be signed was created by the owner of the private key and that it has not been subsequently tampered.

issuance. Therefore, the electronic cash is processed along with the data that includes information about the owners. For details, refer to BOX 2.

(1) The service provider requests the user's certificate and verifies its validity. The certificate's validity is checked against the Certificate Revocation List (CRL) maintained by the certification authority.

(2) The service provider issues electronic cash corresponding to the amount requested by the user[21]. A serial number is assigned to the electronic cash, and the serial number of the issued electronic cash is added to the Issued Electronic Cash Database(DB). Furthermore, a transfer record is attached to each electronic cash instance to indicate that it has been issued (transferred) by the service provider to the user.

(3) The user verifies the service provider's certificate and confirms that the electronic cash and transfer record have been correctly generated (i.e., that the electronic cash has not been forged or tampered with, that the electronic cash and transfer record correspond to the same serial number, and that the user has been specified as the recipient). The electronic cash is then stored on the user's device.

(iii) Transmission of electronic cash

Users can send electronic cash to other users or to stores. During transmission, the recipient's information is added to the transfer record to prevent duplication and double spending (refer to BOX 2 for details).

(1) The user requests the recipient's certificate and verifies its validity[22].

(2) The user adds the recipient's information to the transfer record of the electronic cash, then sends the electronic cash, the updated transfer record, and their own certificate to the recipient.

(3) The recipient verifies the sender's certificate and confirms that the received electronic cash and transfer record have been properly transmitted (i.e., that the electronic cash has not been forged or tampered with, that the electronic cash and transfer record correspond to the same serial number, that the electronic cash is not a duplicate of someone else's, and that the recipient has been specified as the intended recipient). The recipient also checks the accuracy of all transfer records generated since issuance by the service

[21] In this electronic cash system, the face value of the issued electronic cash is fixed. If it is the same as physical cash, there are 10 kinds of denominations (10,000 yen, 5,000 yen, 2,000 yen, 1,000 yen, 500 yen, 100 yen, 50 yen, 10 yen, 5 yen, and 1 yen).

[22] Certificate validation verifies that the counterpart user is the correct user enrolled with the certification authority and that the certificate is valid. To verify the latter, the certification authority must check the Certificate Revocation List (CRL). If it is possible to connect to the Internet, the latest CRL can be checked. Otherwise, it is necessary to set the specification so that the CRL is automatically downloaded to the device as soon as it is connected to the Internet.

provider[23]. The electronic cash and transfer records are then stored on the recipient's device.

(iv) Redemption of electronic cash

To enable retrospective verification of double spending and reissuance of electronic cash, electronic cash must periodically be returned to the service provider[24]. Redemption by the service provider may occur during user refund (cashing out) or be enforced when the number of transfers exceeds a specified limit[25].

(1) The user sends the electronic cash and its transfer record to the service provider.

(2) The service provider verifies that the electronic cash and its transfer record have been correctly transmitted. During this verification, the provider ensures that all transfer records since issuance have been accurately generated and checks the validity of the public keys in the transfer record by referring to the CRL.

(3) The service provider performs a double-spending check (described below).

(4) If the user requests reissuance of the electronic cash, the service provider issues new electronic cash equivalent to the same amount.

(v) Double-spending check for electronic cash

The service provider verifies whether double spending has occurred by checking the serial numbers of redeemed electronic cash.

(1) The service provider references the Issued Electronic Cash DB to check whether the serial number of the redeemed electronic cash exists in the database.

---

[23] This is done to confirm that there is no falsification or inconsistency in the data. If there is falsification or inconsistency, the recipient shall refuse to receive the electronic cash. Since the certificates of other users in the transfer record are not confirmed, even if a user who has not registered with the service provider (without a certificate) or a user who has used a private key stolen from others (the private key corresponding to the public key posted in the CRL) is included in the transfer record, this cannot be detected. Even if such an unauthorized user has engaged in double spending, the service provider cannot identify the user because it does not have the information of the user. However, a user who uses the correct application should not be able to transact with a user who does not have a certificate (the application will reject the transaction). Therefore, it is highly likely that the user who sent electronic cash to the unauthorized user or the user who received electronic cash from the unauthorized person is an accomplice. As a result, service providers may be able to track double spenders by identifying the users involved in the fraud.

[24] Since the size of the transfer record attached to the electronic cash increases in proportion to the number of transfers, it is desirable to recover and reissue electronic cash that has been transferred more frequently.

[25] In Nakayama *et al*. [1997], since the institution issuing the electronic cash is a financial institution, it is possible to check the double spending of electronic cash returned in the form of deposits in an account. In this method, it is also possible for service providers to cooperate with financial institutions to return electronic cash deposited at financial institutions to the service providers for double-spending checks.

(2) If the serial number is found in the DB, it is removed from the database, and the returned electronic cash and its transfer record are stored in the Redeemed Electronic Cash DB.

(3) If the serial number is not found in the DB, the electronic cash is deemed to have been double spent. The transfer record of electronic cash with the same serial number is retrieved from the Redeemed Electronic Cash DB, and the public key of the user who double spent the electronic cash is identified from the two transfer records.

(4) The service provider sends the public key of the double-spending user to the certification authority, which identifies the user corresponding to the public key[26].

BOX 1: Six phases of the electronic cash system

- **Initial setup**

  (1) Service provider I generates a pair of private and public keys for each denomination and publishes the public key along with a certificate issued by a certification authority. Here, the key pair for a denomination of Y yen is represented as $(\mathrm{sk}_{I(Y)}, \mathrm{pk}_{I(Y)})$.

  (2) Certification authority C generates a private and public key pair and publishes the public key together with its own certificate. The certification authority's key pair is represented as $(\mathrm{sk}_C, \mathrm{pk}_C)$.

- **User registration and certificate issuance**

  (1) User U submits their personal information required for certificate issuance to certification authority C.

  (2) Certification authority C verifies the identity of user U and registers the user information.

  (3) User U generates a pair of private and public keys $(\mathrm{sk}_U, \mathrm{pk}_U)$ and sends the public key $\mathrm{pk}_U$to certification authority C.

  (4) Certification authority C associates public key pk_U with the user information and issues a certificate $\mathrm{Cer}_U \leftarrow \mathrm{Sign}_{\mathrm{sk}_C}(\mathrm{pk}_U)$ to user U. Sign is a signature generation function, and $\mathrm{Sign}_{\mathrm{sk}}(m)$ represents the digital signature of the message m with the private key sk. Since the certificate is digitally signed by the certification authority, its validity is verified by the digital signature verification process $1/0 \leftarrow \mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_U, \mathrm{Cer}_U)$. $\mathrm{Verify}_{\mathrm{pk}}(m, \sigma)$ represents the verification formula of the digital signature σ for the message m, and by using the public key pk, it is possible to confirm that the digital signature σ was generated using the private key corresponding to pk and that the message m has not been tampered with. Verify outputs 1 if σ is the correct signature, and 0 if otherwise.

[26] This requires a separate agreement between the service provider and the certification authority and the prior permission of the user.

- **Issuance of electronic cash**

  Service provider I issues electronic cash equivalent to Y yen to user U.

  (1) Service provider I requests public key pk_U and its certificate Cer_U from user U who wishes to issue electronic cash and verifies the correctness of Cer_U using $\mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_U, \mathrm{Cer}_U)$. The validity of pk_U is also checked by referring to the CRL by the certification authority.

  (2) Service provider I issues electronic cash for the amount requested by user U. When SN_i is used as serial number[27], the electronic cash equivalent to Y yen is represented with service provider I 's digital signature for SN_i: $T_i \leftarrow \mathrm{Sign}_{\mathrm{sk}_{I(Y)}}(\mathrm{SN}_i)$. Also, $\sigma_{i(0)} \leftarrow \mathrm{Sign}_{\mathrm{sk}_{I(Y)}}(\mathrm{SN}_i \parallel \mathrm{pk}_U)$ is generated as the transfer record of T_i, and T_i and $\sigma_{i(0)}$ are sent to user U. The serial number SN_i required for verification of $(T_i, \sigma_{i(0)})$ is also sent. Here, $\parallel$ represents the concatenation and $\sigma_{i(n)}$ represents the n-th transfer record of T_i (counting the issuance as 0). After that, the service provider adds the serial number SN_i to the Issued Electronic Cash DB.

  (3) In addition to verifying the certificate of the service provider, user U confirms that the electronic cash and transfer record $(T_i, \sigma_{i(0)})$ are issued correctly using $\mathrm{Verify}_{\mathrm{pk}_{I(Y)}}(\mathrm{SN}_i, T_i)$ and $\mathrm{Verify}_{\mathrm{pk}_{I(Y)}}((\mathrm{SN}_i \parallel \mathrm{pk}_U), \sigma_{i(0)})$, and if outputs for both are 1, they are stored in the device.

- **Transmission of electronic cash**

  User U sends m items of electronic cash $\{T_i\}_{1 \le i \le m}$ to user V[28].

  (1) User U requests the recipient's (user V) public key pk_V and its certificate Cer_V, verifying Cer_V using $\mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_V, \mathrm{Cer}_V)$.

  (2) When updating the transfer record $\sigma_{i(n)}$, for electronic cash T_i, user U generates the digital signature $\sigma_{i(n+1)} \leftarrow \mathrm{Sign}_{\mathrm{sk}_U}(\sigma_{i(n)} \parallel \mathrm{pk}_V)$. The message part of $\sigma_{i(n+1)}$ includes $\sigma_{i(n)}$ and user V's public key pk_V. User U sends the electronic cash and its transfer record $(T_i, \{\sigma_{i(\ell)}\}_{0 \le \ell \le n+1})$ to user V, along with serial number SN_i required for these verifications, public keys of users in the transfer record, and their own public key and certificate. m items of electronic cash $\{T_i\}_{1 \le i \le m}$ are sent as m sets.

  (3) User V verifies user U's certificate Cer_U using $\mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_U, \mathrm{Cer}_U)$, confirms that the received electronic cash and the transfer record are correct, and saves them in their device. Validity of electronic cash T_i and transfer record $\{\sigma_{i(\ell)}\}_{0 \le \ell \le n+1}$ entails: (1) both T_i and $\sigma_{i(0)}$ are signed by the service provider for SN_i; (2) for $0 \le \ell \le n-1$, $\sigma_{i(\ell+1)}$ is the signature for $\sigma_{i(\ell)}$ and the user's public key, whose signer is the user corresponding to the public key in the message portion of $\sigma_{i(\ell)}$; and (3) $\sigma_{i(n+1)}$ is the sending user U's

[27] The index i *is* the serial number when dealing with multiple electronic cash.

[28] Since electronic cash is issued in face value unit (footnote 21), it should be counted by the number of items when transmitting.

signature for $\sigma_{i(n)}$ and their own public key.

Further, in (1), for a user's public key pk, it holds that $1 \leftarrow \mathrm{Verify}_{\mathrm{pk}_{I(Y)}}(\mathrm{SN}_i, T_i)$ and $1 \leftarrow \mathrm{Verify}_{\mathrm{pk}_{I(Y)}}((\mathrm{SN}_i \parallel \mathrm{pk}), \sigma_{i(0)})$, and in (2), for $0 \leq \ell \leq n-1$, it holds that $1 \leftarrow \mathrm{Verify}_{\mathrm{pk}}((\sigma_{i(\ell+1)} \parallel \mathrm{pk}'), \sigma_{i(\ell+2)})$ and $1 \leftarrow \mathrm{Verify}_{\widetilde{\mathrm{pk}}}((\sigma_{i(\ell)} \parallel \mathrm{pk}), \sigma_{i(\ell+1)})$, for a user's public key pk. Here, pk' is the public key of the user to whom the user with public key pk sent T_i, and $\widetilde{\mathrm{pk}}$ is the public key of the user who sent T_i to the user with public key pk. Also, in (3), it holds that $1 \leftarrow \mathrm{Verify}_{\mathrm{pk}_U}((\sigma_{i(n)} \parallel \mathrm{pk}_V), \sigma_{i(n+1)})$.

- **Redemption of electronic cash**

(1) User V sends the electronic cash, its transfer record $(T_i, \{\sigma_{i(\ell)}\}_{0 \leq \ell \leq n+1})$, serial number SN_i, user public keys in the transfer record, and their own public key and certificate to the service provider.

(2) The service provider I confirms that the received $(T_i, \{\sigma_{i(\ell)}\}_{0 \leq \ell \leq n+1})$ is correct. The validity of public keys in the transfer record is confirmed via the certification authority's CRL.

- **Double-spending check for electronic cash**

(1) Service provider I refers to the Issued Electronic Cash DB to check whether the serial number SN_i for the redeemed electronic cash T_i is in the DB.

(2) If SN_i exists, it is removed from the Issued Electronic Cash DB and the returned electronic cash, along with its transfer record, is added to the Redeemed Electronic Cash DB.

(3) If SN_i does not exist, double spending is suspected. The service provider retrieves the electronic cash and transfer records with the same SN_i from the Redeemed Electronic Cash DB and identifies the double-spending user from the two transfer records. For instance, for two transfer records with the same serial number, if one transfer shows recipient pk_{U_2} the other pk_{U_3}, the user associated with public key pk_{U_1} is identified as the offender.

(4) The service provider reports the offending user's public key to the certification authority, which identifies the corresponding user.

BOX 2: Measures against forgery, tampering, duplication, and double spending of electronic cash

- **<u>Measures against forgery and tampering of electronic cash</u>**

(To prevent the forgery of electronic cash by entities other than the issuing authority, as well as the tampering of amounts or ownership information by entities other than

the issuing authority): Electronic cash T is represented as digital signature $T \leftarrow \mathrm{Sign}_{\mathrm{sk}_I}(\mathrm{SN})$ created by the issuing authority I for the serial number SN. Digital signature technology prevents forgery and tampering of electronic cash by third parties.

- **Measures against duplication of electronic cash by third parties**
  (To prevent fraud involving the duplication and use of electronic cash owned by others): The correspondence between electronic cash and its owner prevents third parties from duplicating and using electronic cash fraudulently. Specifically, by adding the public key of the user to the transfer record of electronic cash in a tamper-resistant format, only the corresponding user is able to use the electronic cash[29].

- **Measures against double spending of electronic cash across multiple users**
  (To prevent fraud where the legitimate owner duplicates received electronic cash and uses it by sending the duplicated cash to multiple users): Since the generation of a signature using a private key is required when sending electronic cash, fraud can be prevented through the tamper resistance of the device. However, as technological advancements may reduce the tamper resistance of devices, it is essential to prepare for such situations (see section (4) of this chapter). To address this, electronic cash is accompanied by its transfer record in a tamper-resistant format so that service providers can retrospectively identify fraudulent users.

  - For example, if two instances of electronic cash with the same serial number SN_i are detected and are as follows: For $\sigma_{i(\ell-1)}(=\mathrm{Sign}_{\mathrm{sk}_{U_1}}(\sigma_{i(\ell-2)} \parallel \mathrm{pk}))$, if the public key contained in the message section is pk_{U_2} in one instance and pk_{U_3} in the other instance, it can be determined that the signer of $\sigma_{i(\ell-1)}$ (the user corresponding to public key pk_U) sent the same electronic cash to two different users (pk_{U_4} and pk_{U_5} are the following users' public keys).

$$\sigma_{i(\ell)} = \mathrm{Sign}_{sk_{U_2}}(\mathrm{Sign}_{sk_{U_1}}(\sigma_{i(\ell-2)} \parallel pk_{U_2}) \parallel pk_{U_4})$$
$$\sigma_{i(\ell)} = \mathrm{Sign}_{sk_{U_3}}(\mathrm{Sign}_{sk_{U_1}}(\sigma_{i(\ell-2)} \parallel pk_{U_3}) \parallel pk_{U_5})$$

- **Measures against duplication of electronic cash for the same user**
  (To prevent fraud where the legitimate owner or a third party duplicates electronic cash and uses it by resending it to the same user): This can be addressed by adding one-time attributes, such as time stamps, to the transfer record, or by implementing the transmission process of electronic cash as a challenge-response mechanism[30].

[29] An attacker can duplicate electronic cash by eavesdropping the communication channel between users or by illegally reading it from the device.

[30] A method that uses randomly generated values by the verifier each time to counter replay attacks. A replay attack is a type of attack where intercepted data from a communication channel is reused to impersonate a legitimate party. The random value sent by the verifier is called the challenge, and the response provided by the prover is called the response.

(4) Considerations on security

(i) Tamper resistance of devices

The security of electronic cash systems largely depends on the security of digital signatures, and as such, the use of devices capable of securely managing the private keys used for digital signatures is a prerequisite. A tamper-resistant device makes it difficult even for its legitimate owner to illicitly extract the private key stored within or to tamper with the application. This ensures that fraud, such as double spending of electronic cash, can be prevented. However, malicious users may deliberately use non-tamper-resistant devices to commit fraud. Therefore, service providers may need to verify the tamper resistance of user devices. For example, user registration could be allowed only if the tamper resistance of the user's device is confirmed, thereby excluding users who attempt fraud.

Nonetheless, as attack techniques against device security mechanisms evolve, tamper resistance may degrade over time. In such a scenario, even if the aforementioned measures are implemented, it may no longer be possible to prevent double spending of electronic cash. Additionally, service providers design their applications based on the assumption that the security features built into devices will function as expected. However, cases where these features fail to operate as intended make it difficult to conduct proper risk assessment and management of applications, as noted by Isobe and Une [2021]. To address the potential degradation of tamper resistance, electronic cash systems incorporate transfer records in a tamper-resistant format within electronic cash itself. By checking the serial numbers of circulated electronic cash, service providers can retrospectively detect double spending by users[31].

(ii) Relationship between users, devices, and keys

To prevent fraud such as the unauthorized duplication and use of electronic cash by others, electronic cash is designed to be usable (e.g., transferable to other users) only with the "private key" linked to the electronic cash. In this context, the relationship between the "user (person)" and the "device" storing the private key can be classified into the following patterns:

[31] One of the methods for conducting electronic payments is called the "balance management scheme," which is similar to that adopted in electronic money, where monetary value received from other users is aggregated, stored, and managed within a device for making payments. However, even in the balance management scheme, if tamper resistance is compromised, it becomes possible to manipulate the data within the device fraudulently and use it to create unlimited monetary value. To detect such fraud retrospectively, it is necessary to manage all transactions using a server-side ledger (Soyama [2020]).

- Case A: Anyone in possession of the device can use the electronic cash stored in it (an *n*-to-1 relationship).
- Case B: Only the legitimate owner of the device can use the electronic cash stored in it (a 1-to-1 relationship).

Case A resembles the use of physical cash and may seem to offer higher usability. However, to ensure post-fraud detection and transparency of electronic cash, the system assumes the use of Case B. In Case B, electronic cash is tied to the "user (person)," allowing only the corresponding user to utilize the electronic cash. To implement Case B, methods such as restricting device usage to its legitimate owner or adopting a mechanism where only the owner can generate the private key may be employed[32].

(5) Considerations on privacy protection and transparency

(i) Balancing privacy protection and transparency

There is a prevailing opinion that payment services must account for users' privacy. For instance, the Financial Research Study Group [2018] identified that one of the conditions for the acceptance of new payment methods is that they should provide a level of safety and security equivalent to physical cash. It recommends that service providers strive to protect privacy and personal information.

On the other hand, from the perspective of AML/CFT, there may be cases where it is necessary to retrospectively trace the flow of funds. In such cases, ensuring traceability becomes critically important (Noda [2022]). While physical cash lacks traceability, its physical constraints in storage and circulation somewhat limit its use as a medium for money laundering. However, given the risks associated with electronic transfer and payment methods as potential media for money laundering, measures that enable retrospective tracking are essential.

As such, achieving a balance between privacy protection and transparency is crucial for businesses providing payment services. The following discussion addresses privacy protection for users against other users and against service providers, respectively.

[32] For example, a private key may be generated each time from the biometric information of the user using Public Biometric Infrastructure (PBI) (Takahashi [2021]).

(ii) Privacy protection against other users

As summarized in section (3) of this chapter, during the transmission and receipt of electronic cash, the sending and receiving users verify each other's certificates. Consequently, if personally identifiable information (such as name or address) is included in a certificate, it could enable identification of the counterpart user[33]. In cases such as payments at retail stores, where identifying the counterpart user is unnecessary, certificates should ideally exclude personally identifiable information.

Additionally, electronic cash is transmitted and received along with its transfer record, which includes the public keys of users who previously owned the cash. Even if the public key (or certificate) does not contain personally identifiable information, the public key itself could serve as a user ID, enabling the association of various pieces of information. For instance, if information about the transaction counterpart is obtained through a separate channel (e.g., face-to-face payment), it would become possible to identify the relationship between a user and their public key, potentially enabling the identification of connections among the electronic cash instances used by the user. To ensure anonymity and unlinkability of electronic cash, public keys should be updated for each transaction (Nakayama *et al*. [1997])[34]. Furthermore, cryptographic techniques known as zero-knowledge proofs could be employed to prove ownership of electronic cash without disclosing the certificate itself. Protocols utilizing zero-knowledge proofs are discussed in Chapter 4.

(iii) Privacy protection and transparency for service providers

When issuing electronic cash, service providers verify the certificates of users receiving the cash. However, by ensuring that personally identifiable information is not included in the certificates, users' privacy can be safeguarded as long as the service provider does not collude with the certification authority.

Moreover, since electronic cash transactions occur exclusively between users, service providers cannot access transaction details in real time. While service providers may verify the

[33] It is possible to design the application in a way that does not disclose the content of received data to the user. However, with a certain level of technical skill, it is possible to duplicate data transmitted between smartphones. Therefore, it is important to consider the potential impact that transmitted and received data may have on users' privacy.

[34] There are other methods (for example, Chaum [1983]) to protect users' privacy by using electronic cash only once, but they do not satisfy the need to freely transfer electronic cash.

transfer record of electronic cash upon redemption, the only information available from the transfer record is the public key of users. Without collusion with the certification authority, it is not possible to identify individual users, thus preserving the anonymity of electronic cash.

As a means of strengthening measures against fraud at certification authorities, separating the functions of user information management and certificate issuance could be considered. For details on certificate issuance methods under such functional separation, refer to Appendix 1. Additionally, it is technically possible to ensure that users who double spend electronic cash can be identified from redeemed electronic cash, while ensuring that no information is revealed about other users. Methods for enhancing privacy protection for service providers are discussed in Chapter 4.

As noted in section (5) (ii) of this chapter, transaction counterparts may have the potential to associate a user with their public key. Thus, by colluding with such a transaction counterpart, service providers could identify a user's transactions based on redeemed electronic cash. To meet the requirements of anonymity and unlinkability of electronic cash even in such cases of collusion, it is necessary, as with the privacy protection measures for other users, to update public keys for each payment transaction.

From the perspective of transparency, it is desirable to periodically review the transfer record of electronic cash. For instance, a design could be adopted where electronic cash is returned to the service provider if it exceeds x transfers or after y periods since issuance. Such measures would enable the service provider to monitor suspicious activities related to electronic cash. Furthermore, in cases such as high-value transfers, where it is necessary to collect real-time information, one possible measure is to permit high-value transfers only when an Internet connection is available, while automatically transmitting a copy of the electronic cash transaction from the application to the service provider. Additionally, by creating a block list for electronic cash, the circulation of cash with suspicious records could be restricted. These measures can be implemented using the programmability embedded in electronic cash.

3. Practical evaluation of electronic cash systems

(1) Past demonstration experiments

Demonstration experiments based on electronic cash systems have been conducted multiple times in the past. These experiments primarily involved storing electronic cash on contact-based

IC cards and sending it via the Internet to stores or other users. The electronic cash was issued by financial institutions in the form of withdrawals from deposit accounts and could be used in both virtual (Internet-based) and physical stores. The purpose of these experiments was to examine whether such electronic cash scheme could function as a new payment method to replace physical cash and to identify challenges for its practical implementation as a service.

- Internet Cash (1998)

The demonstration experiment for Internet Cash (September 1998 – February 2000) was conducted with the cooperation of four financial institutions and approximately 10,000 participants from the general public. Internet Cash, stored on IC cards, could be used for payments to virtual stores or transfers to other users via reader-writers connected to personal computers. Additionally, Internet Cash could be circulated among users. Internet Cash issued by financial institutions could also be refunded to deposit accounts (Cyber Business Council [2000]).

- Super Cash (1999)

The Super Cash demonstration experiment (April 1999 – May 2000) involved the cooperation of 24 financial institutions, approximately 1,000 stores, and about 22,000 participants. As this experiment focused on usability in real-world scenarios, Super Cash was usable not only in virtual stores but also in physical stores. Users could also recharge their IC cards using charge machines installed at financial institutions or via public telephones. However, the Super Cash used in stores was designed to transmit data to a central data center, and its transferability was not evaluated in this experiment (NTT Communications Corporation [2000]).

While the demonstration experiments for Internet Cash and Super Cash provided overviews of their respective implementations, they did not document the time required for transmitting and receiving electronic cash. Considering the IC card specifications and communication environments at that time, it is presumed that ensuring usability posed significant challenges.

(2) Overview of the practical evaluation

Approximately 25 years have passed since the aforementioned demonstration experiments, and the technological environment surrounding us has changed significantly[35]. Therefore, this study seeks to evaluate the usability of electronic cash system based on current technological standards. In this evaluation, the focus is placed on the transmission processing of electronic cash as a starting point for the study of implementing the electronic cash system. Although comprehensive usability evaluation also includes factors such as application operability, this study evaluates usability primarily based on the time required to transmit electronic cash.

(i) Specifications of devices used

To implement electronic cash system, devices need to include tamper-resistant hardware for storing sensitive information such as private keys, as well as communication capabilities for transmitting and receiving electronic cash. Since smartphones are equipped with an embedded Secure Element (eSE) as tamper-resistant device [36] and offer multiple communication functionalities such as mobile data, Wi-Fi[37], Bluetooth[38], and Near Field Communication (NFC), this evaluation assumes the use of smartphones. As of 2024, smartphones have an adoption rate of 97% in Japan (NTT Docomo Mobile Society Research Institute [2024]), making them a widely used device. The cryptographic algorithm used for the electronic cash system is ECDSA (Certicom Research [2000]), a cipher recommended for e-government.

---

[35] In 2000, the Internet usage rate was 37.1%, and telephone dialup was the predominant method. The Asymmetric Digital Subscriber Line (ADSL), which began commercial service in 2000, had a maximum transmission speed of 50 megabits per second downstream and 5 megabits per second upstream. On the other hand, the Internet usage rate in 2023 was 84.9%, and the maximum communication speed of the fifth-generation mobile communication system (5G) launched in 2020 was 4.2 gigabits per second downstream and 218 megabits per second upstream, 84 times and about 43 times higher than ADSL, respectively. The high-performance IC card developed by NTT Corporation around 1999 had a central processing unit (CPU) clock frequency of 15 megahertz, a random-access memory (RAM) capacity of 2 kilobytes, and a flash memory capacity of 512 kilobytes. In contrast, the current general smartphone has a multi-core structure with a CPU clock frequency of several gigahertz, with RAM capacity of several gigabytes and flash memory capacity of several hundred gigabytes. Many of these devices have built-in SEs, which have tamper resistance similar to IC cards. The ST54K (manufactured by ST Microelectronics), the eSE used in the 2022 smartphone (Google Pixel 7), has a CPU clock frequency of 100 megahertz, 64 kilobytes of RAM, and 2,048 kilobytes of flash memory. Google Pixel is a trademark or registered trademark of Google LLC.

[36] As of 2024, about 90% of Android smartphones sold in Japan are equipped with GP-SE. GP-SE refers to an SE that complies with the standard specifications of the Global Platform, which promotes the standardization of IC card technologies.

[37] Wi-Fi is a registered trademark of the Wi-Fi Alliance.

[38] Bluetooth is a registered trademark of Bluetooth, SIG Inc.

(ii) Assumptions for the practical evaluation

(a) Transaction response time

The time required for processing electronic cash transmission (turnaround time) is defined as the time from selecting the recipient and entering the transfer amount on the application menu screen to the completion of the transfer. Of this, the time from pressing the "Send" button to the transition to the transfer completion screen is the total of the processing time on the sender's and recipient's smartphones and the data communication time (referred to as the transaction response time) (Figure 3). Specifically, this includes: (1) the time required to update the transfer record (signature generation), (2) the time required for the transmission of electronic cash, and (3) the time required to verify the electronic cash and transfer record (signature verification).

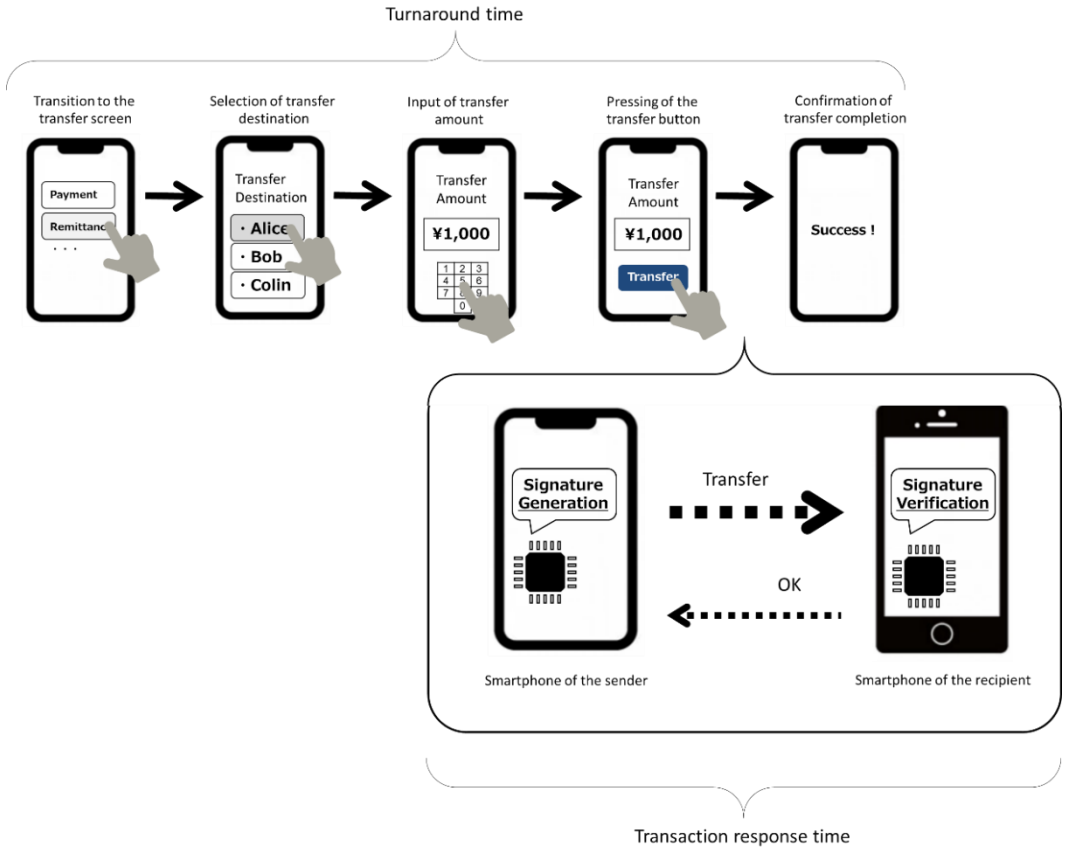


Figure 3: Operations related to electronic cash processing

(b) Processing for signature generation and verification

For updating the transfer record (1), the sender first verifies the recipient's certificate and then generates a digital signature. If the sender is transmitting m items of electronic cash[39], m items of signature generation processing are required. Letting the processing times for certificate verification and signature generation per item be t_{vs} and t_s (seconds), respectively, the time required for transmission processing is $t_{vs} + t_s \cdot m$ (seconds). For the verification of electronic cash and transfer record (3), the recipient verifies the sender's certificate and the transfer record (digital signature verification). If the number of post-issuance transfers for m items of electronic cash is n_m for each item, and the processing time per item for signature verification is t_v (seconds), the time required for reception processing is $t_{vs} + t_v \cdot \sum_m (n_m + 1)$ (seconds). Thus, the total time for (1) and (3) in a single transaction is $2t_{vs} + t_s \cdot m + t_v \cdot \sum_m (n_m + 1)$ (seconds).

To optimize the implementation of electronic cash system, a hybrid architecture is envisaged, in which only signature generation processing, which requires private keys, is performed on tamper-resistant devices such as SEs, while signature verification processing, which does not require private keys, is performed in isolated execution environments such as TEEs. Comparing the processing capabilities of each execution domain, the isolated execution environment can use the same computing resources as the normal environment, while the tamper-resistant devices (especially the eSEs installed in smartphones) have low computing power per unit of time due to the limited computing resources available[40] and incur additional overhead for calls from higher layers.

Since digital signature generation involves more computation than signature verification, the signature generation process is likely to be the bottleneck in performance when implemented on tamper-resistant devices. Therefore, this study focuses on the time required for signature generation (t_s).

[39] It is assumed that the system is programmed to send at a minimum number of items depending on the amount to be remitted.

[40] According to specification sheets of eSEs available in the market as of 2024,, CPU clock frequencies are in the order of 10 to 100 megahertz (single core), and RAM is in the order of 10 to 100 kilobytes, which result in lower computing power compared to normal or isolated execution environments.

(c) Processing for electronic cash transmission

Among the communication functions built into smartphones, short-range communication can still function during disasters or communication outages. Ensuring payment functionality even in environments where the Internet is inaccessible is one of the requirements for electronic cash (Chapter 2 (2), property (7)). Therefore, this evaluation uses short-range wireless communication technology to transmit electronic cash. It is expected that if usability can be confirmed for face-to-face payments, usability for payments using faster Internet communication can also be assured.

Modern smartphones are generally equipped with Bluetooth, Wi-Fi Direct[41], and NFC as standard features (see Table 4) Bluetooth is a short-range communication standard with a range of approximately 10 meters and is primarily used to wirelessly connect peripheral devices to smartphones. Bluetooth includes two variations: Bluetooth Classic, which supports high-speed transmission of large amounts of data, and Bluetooth Low Energy (Bluetooth LE), characterized by low data transfer speeds and ultra-low power consumption. Wi-Fi Direct is a standard that enables devices equipped with Wi-Fi functionality, such as PCs and smartphones, to connect wirelessly to one another without the need for a wireless LAN router. NFC is a short-range wireless communication technology with a range of about 10 centimeters, enabling communication between contactless IC cards and devices, as well as device-to-device interaction.

[41] Wi-Fi Direct is a trademark or registered trademark of the Wi-Fi Alliance.

	Short-range wireless communication technologies			
	Bluetooth Classic	Bluetooth Low Energy	Wi-Fi Direct	NFC
Maximum transmission rate specification (per second)	3 megabits (EDR PHY (8DPSK))	2 megabits (LE 2M PHY)	9.6 gigabits (Wi-Fi 6)	106 kilobits (Type-A/B) 424 kilobits (Type-F)
Connection between iOS[*1] and Android[*2]	Not possible[*3]	Possible	Possible[*4]	Possible
Connection authentication	Required	Not required	Required	Not required
Encryption of communication data	Yes	Yes (if connection is authenticated)[*5]	Yes	No[*6]

Notes:
[*1] iOS is a trademark or registered trademark of Cisco Systems, Inc. in the United States and/or other countries.
[*2] Android is a trademark of Google LLC.
[*3] As of June 2024.
[*4] Must be designed so that the Android side becomes the group owner.
[*5] Possible to design encryption at the application layer even when connection authentication is not performed.
[*6] Possible to design encryption at the application layer.

Table 4: Comparison of short-range wireless communication technologies

When comparing these technologies, NFC is widely used for electronic money transactions and similar applications but has slower communication speeds compared to Bluetooth and Wi-Fi Direct[42]. Furthermore, Bluetooth Classic differs in supported profiles between iOS and Android, and as of the time of writing (October 2024), cross-platform[43] communication between applications is not feasible. Consequently, to enable the transmission and reception of electronic cash between smartphones of different models, Bluetooth Low Energy and Wi-Fi Direct are considered viable options.

[42] If the data size per electronic cash item is about 4 kilobytes, the data size for sending 50 electronic cash is about 200 kilobytes (= 1.6 megabits). The theoretical maximum transmission bandwidth for NFC is 424 kilobits per second, which means it would take about 3.8 seconds to send 50 items.
[43] A program that runs applications with the same specifications on different operating systems (OSs).

(3) Results of the practical evaluation

(i) Time for signature generation

The time required for generating one digital signature using ECDSA was measured using evaluation boards for three types of eSEs[44]. The results showed significant variation depending on the chip vendor and version: 112 milliseconds for Company A, 102 milliseconds for Company B (Version 1), and 35 milliseconds for Company B (Version 2) (Table 5). With the fastest eSE from Company B (Version 2), theoretically, it would take less than 1.0 second to generate all signatures (update the transfer record) for 28 items of electronic cash.

	Types of eSEs		
	Company A	Company B (Version 1)	Company B (Version 2)
Signature generation time	112 milliseconds	102 milliseconds	35 milliseconds

Table 5: Comparison of signature generation time (Average time of 50 attempts)

On the other hand, there may be a need to send larger amounts of electronic cash in one transaction. For larger-scale transactions, a method introduced in Chapter 4 (1) constructs a Merkle tree with messages to be signed as leaves and applies a signature only to the root value (root hash). Using this method, regardless of the number of items transmitted, the number of signature generations required for updating the transfer record can be reduced to one. For Company B's (Version 2) eSE, this means the signature generation time remains 35 milliseconds, irrespective of the number of items sent.

(ii) Time for electronic cash transmission

The evaluation measured the time required to transmit electronic cash using Bluetooth Low Energy and Wi-Fi Direct with an Android smartphone. The transmission times were measured for 1, 50, and 100 items of electronic cash, excluding the time required for establishing connections.

[44] The eSEs used in the verification were products of two major chip vendors (Company A and Company B). Company B (Version 2) is a successor to Company B (Version 1).

The results showed that for transmitting 100 items, Bluetooth Low Energy took 10.7 seconds (10,700 milliseconds), while Wi-Fi Direct completed the transmission in just 0.16 seconds (160 milliseconds). This confirms that Wi-Fi Direct is more efficient for transmitting electronic cash (Table 6).

		Delivery size (Bytes)	Transmission time in milliseconds (not including connection establishment time)	
			Bluetooth Low Energy	Wi-Fi Direct
No. of items	1	3,380	590	2
	50	169,000	5,580	62
	100	338,000	10,700	160

Note:* Size of electronic cash and transfer record assuming 5 transfers since issuance. Since the size of the electronic cash (signed by the service provider) is 580 bytes and the transfer record is 560 bytes, the total is 580 + 560*5 = 3,380 bytes. The test data for evaluation were prepared by estimating the size as follows. Data related to electronic cash T: 580 bytes = signature size 96 bytes + message size 484 bytes (public key, serial number, etc.); data related to transfer record σ: 560 bytes = signature size 96 bytes + message size 464 bytes (public key, etc.)

Table 6: Electronic cash delivery time comparison (Average time of 50 attempts)

(iii) Transaction response time

Using Company B's (Version 2) eSE and leveraging Merkle tree-based optimization, the signature generation time for sending 100 items of electronic cash can be reduced to 35 milliseconds. Assuming a similar time for signature verification at the recipient's end, the total processing time for both the sender's and recipient's applications would be approximately 70 milliseconds. Since Wi-Fi Direct enables transmission to the recipient in 160 milliseconds, the total transaction response time for sending 100 items of electronic cash is approximately 230 milliseconds (0.23 seconds).

A study suggests that a transaction response time of less than 1.0 second is desirable (Nielsen [2010]). Compared to credit card contactless payments (0.5 seconds, Visa [2014]) or public transportation e-money payments (0.2 seconds, Ootsuki [2011]), a response time of 0.23 seconds is evaluated as offering sufficient usability. However, unlike contactless payments, electronic cash system involves smartphone operation and requires connection authentication and encryption for Wi-Fi Direct, necessitating further consideration of the time required for these processes.

4. Considerations for enhancing the efficiency of electronic cash systems

This chapter discusses methods to improve the efficiency of the processes involved in sending and receiving electronic cash, as well as the redemption of electronic cash. Specifically, the focus is on two aspects: (1) a method for batch processing the update of transfer records when transmitting multiple electronic cash, and (2) an efficient method to verify digital signatures issued by the same signer during the redemption process, which is conducted by service providers.

In addition, under the electronic cash system described in Chapter 2, if the user does not possess the exact amount of electronic cash required for a transaction, they need to receive change. This means that in a fixed-denomination electronic cash system, two transfer processes are often necessary for a single transaction. Therefore, as a method to enhance efficiency, this chapter considers a variable-denomination system, which allows users to flexibly split and aggregate their electronic cash for transmission (Chapter 2 section (2), property (2)). Although variable-denomination systems have been studied in the past (e.g., Okamoto and Ohta [1992]), the approach here differs from existing methods by employing digital signature algorithms (e.g., ECDSA or EdDSA[45]) as components. This configuration allows the use of arbitrary signature algorithms and offers flexibility, such as adaptability to cryptographic migration challenges[46].

Furthermore, under the electronic cash system described in Chapter 2, users were required to update their public keys for each transaction to ensure unlinkability. This chapter proposes a method to satisfy unlinkability using zero-knowledge proofs, thereby streamlining the process of updating public keys.

(1) Enhancing the efficiency of electronic cash transmission and receipt

From a usability improvement perspective, this section explores ways to optimize the process of sending electronic cash. Under the electronic cash system in Chapter 2, the transfer record of each item of electronic cash being sent need to be individually updated. Since the transfer

[45] EdDSA is one of the e-Government recommended ciphers. It is a digital signature scheme using the Edward curve.

[46] It should be noted, however, that when the signature size is drastically changed, such as in quantum-resistant cryptography, it is necessary to change the message size in the communication protocol. In the financial field, studies on the transition to quantum-resistant computer cryptography are progressing (Une [2023]), and it is important to make the configuration aware of the future transition to cryptography.

record must be secured with digital signatures to prevent tampering, the processing time for sending electronic cash increased in proportion to the number of items being sent.

To address this, the following protocol introduces the use of Merkle trees to improve the efficiency of digital signature generation. A Merkle tree is a tree structure where each leaf node is labeled with the hash value of data, and each internal node is labeled with the hash value of its child nodes' labels. In this method, a signature is generated for the root value (root hash) of the Merkle tree constructed from the transfer record of the electronic cash being sent. As a result, the number of signature generations required can be reduced to one, regardless of the number of items being sent (Figure 7).

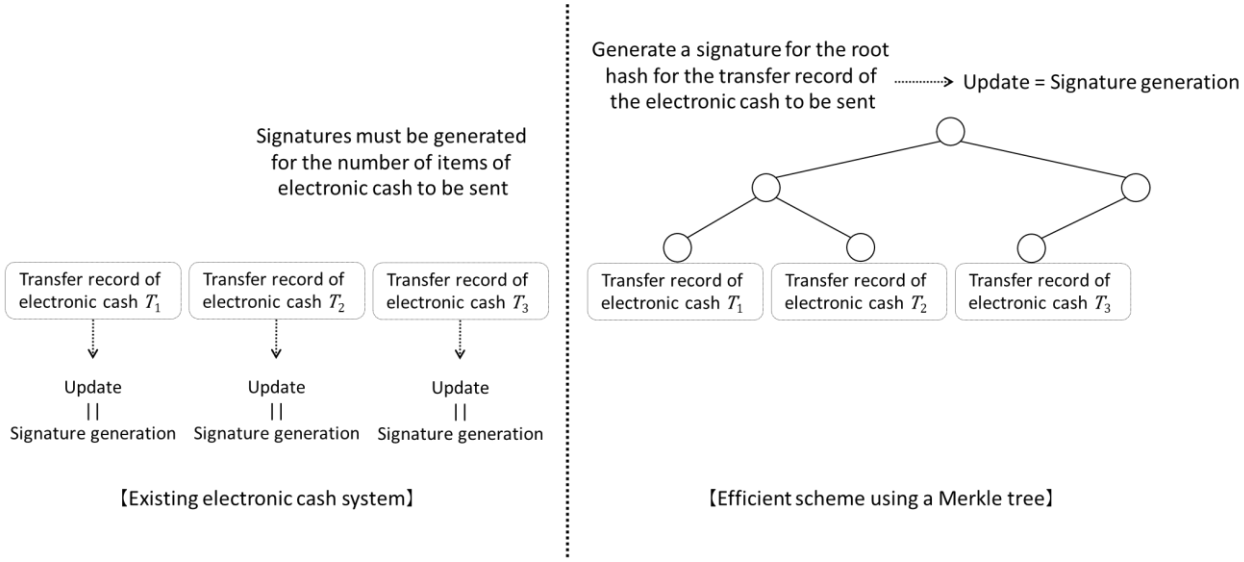


Figure 7: Efficient scheme using a Merkle tree

The process for transferring electronic cash from user U to user V is as follows:

(1) User U requests a certificate Cer_V from the recipient user V and verifies its validity.

(2) When sending m items of electronic cash $\{T_i\}_{1\le i\le m}$, with serial number SN_i, user U calculates $h_i \leftarrow H(\sigma_{i(n_i)})$ $(1 \le i \le m)$ for the transfer records $\{\sigma_{i(\ell)}\}_{1\le i\le m, 0\le \ell\le n_i}$. Here, n_i represents the number of transfers that the electronic cash T_i has undergone, and $\sigma_{i(\ell)}$ represents the ℓ-th transfer record of T_i. The initial transfer record at the time of issuance of T_i is $\sigma_{i(0)}$. Additionally, user U constructs a Merkle tree L with $\{h_i\}_{1\le i\le m}$ as leaf nodes and computes the root value h (refer to Appendix 2 (1) for details on constructing a Merkle tree).

(3) To update the transfer record, user U generates a digital signature $\sigma \leftarrow \mathrm{Sign}_{\mathrm{sk}_U}(h \parallel \mathrm{pk}_V)$ for h and user V's public key pk_V. Note that sk_U is the private key of user U.

(4) User U sends the electronic cash with the updated transfer record to user V. The data sent includes $\{\mathrm{SN}_i, T_i, \sigma, \sigma_{i(\ell)}\}(1 \leq i \leq m, 0 \leq \ell \leq n_i)$ and the public keys in the transfer record.

(5) User V verifies the validity of the electronic cash using the digital signature and stores the received electronic cash in their device.

Through this protocol, user V, the recipient of the electronic cash, only needs to perform a single signature verification for the transfer record updated by user U, regardless of the number of electronic cash received. However, previous transfer records $\sigma_{i(\ell)}(0 \leq \ell \leq n_i)$ still require verification as before. For details on this protocol, refer to Appendix 3.

(2) Enhancing the efficiency of electronic cash redemption

During redemption, service providers must verify that all transfer records of the redeemed electronic cash have been correctly generated since issuance. If the electronic cash has been transferred n-th times since issuance, the transfer record will contain $n + 1$ linked digital signatures, all of which must be verified. As the number of redeemed electronic cash increases, the processing load on the service provider also increases proportionally.

In the EdDSA signature scheme, the number of elliptic curve multiplications required during signature verification can be reduced by linearly combining multiple verification equations from the same signer (Bernstein *et al*. [2012], Fujisaki [2020]). The processing load for verifying transfer records can be reduced by aggregating the signatures of large-scale users, such as financial institutions or retailers, within the redeemed transfer records[47]. For further details on the EdDSA algorithm, refer to Appendix 2 (2).

(3) Considerations for a variable denomination scheme

The electronic cash system discussed in Chapter 2 has fixed denominations, meaning that users cannot split their electronic cash into smaller amounts. This section introduces a method to enable flexible denomination splitting, as well as representing arbitrary amounts with a tree

[47] Comparing the signature verification process that applies batch processing to multiple signatures by the same signer and the signature verification process without batch processing, using an ordinary laptop PC, the execution time when batch processing was applied was about 45% of that when batch processing was not applied (average value for 1 million attempts).

structure whose leaves correspond to the smallest units (e.g., 1 yen). Specifically, a user can create an N-ary tree ($N \geq 2$) where the leaves represent 1 yen, and the service provider issues electronic cash as a digital signature for the root value of this N-ary tree. When a user wishes to send part of their electronic cash, they create a subtree corresponding to the desired amount and send this subtree (with its root value and signature) as electronic cash[48]. Thus, in this scheme, both the electronic cash and its transfer record are updated with each transaction. Additionally, the method introduced in section (1) of this chapter, which uses Merkle trees, can also be applied to reaggregate split electronic cash for transmission.

The following section describes the protocol for issuing and sending electronic cash with $N = 2$, using specific examples[49].

(i) Issuance of electronic cash

A process where a service provider issues electronic cash worth 6 yen to user U is as follows:

(1) The service provider generates a pair of private and public keys $(\mathrm{sk}_I, \mathrm{pk}_I)$ and publishes the public key along with a certificate issued by the certification authority.

(2) The service provider generates a binary tree of depth $3 = (\lceil \log_2 6 \rceil)$ to represent 6 yen and assigns labels to the leaves. The labels represent the position of the leaves in the binary tree, numbered sequentially from left to right as 1, 2, 3, and so forth.

(3) The service provider generates a random number r and assigns it to the root of the binary tree.

(4) The service provider generates serial number $\mathrm{SN}_{(0)} := (r \parallel ¥6 \parallel 1{\sim}6)$ for the electronic cash representing 6 yen[50]. The serial number $\mathrm{SN}_{(n)} := (r \parallel \mathrm{amount} \parallel \mathrm{left}{\sim}\mathrm{right})$ uniquely identifies the tree structure of the electronic cash, consisting of the random number r assigned to the root, the amount, and information specifying the range of the leaves (from the leftmost label left to the rightmost label right) for 6 yen (see Figure 8). Here, n represents the number of transfers of the electronic cash after issuance.

[48] As a method to implement the variable denomination scheme, it is conceivable to include amount information in the message portion of a signature, similar to transactions in Bitcoin. However, this protocol instead transmits electronic cash in units of 1 yen, distinguishable from one another, rather than in monetary values. This allows for the identification of which specific electronic cash were double spent, even in cases where double-spent electronic cash becomes mixed. Notably, Bitcoin uses a ledger-based system, which promptly performs double-spending checks, making it unlikely for double-spent bitcoins to mix at their destination.

[49] The protocol for detection by service providers of double spending of electronic cash is omitted, but as with the existing method, service providers store all redeemed electronic cash and check for duplicates.

[50] In generalization, the serial number is represented as $\mathrm{SN}_{i(0)} := (r_i \parallel ¥6 \parallel 1{\sim}6)$ for a random number r_i.

(5) The service provider generates electronic cash $T_{(0)} \leftarrow \mathrm{Sign}_{\mathrm{sk}_I}(\mathrm{SN}_{(0)} \parallel ¥6)$ representing 6 yen and its transfer record $\sigma_{(0)} \leftarrow \mathrm{Sign}_{\mathrm{sk}_I}(\mathrm{SN}_{(0)} \parallel ¥6 \parallel \mathrm{pk}_U)$, and sends $(\mathrm{SN}_{(0)}, T_{(0)}, \sigma_{(0)})$ to user U. The electronic cash comprises a digital signature on the serial number $(\mathrm{SN}_{(0)})$ and the amount (¥6), and the transfer record includes the recipient user's public key (pk_U).

(6) The service provider registers the issued electronic cash $(T_{(0)})$ in the Issued Electronic Cash DB, ensuring $T_{(0)}$ can be retrieved using r as an index.

(7) User U verifies the validity of the received $(T_{(0)}, \sigma_{(0)})$ by checking the following:

- Both $T_{(0)}$ and $\sigma_{(0)}$ are signatures by the service provider on the same serial number $(\mathrm{SN}_{(0)})$,
- $\mathrm{SN}_{(0)}$ is correctly structured based on the issued amount, and
- $\sigma_{(0)}$ is a signature by the service provider on pk_U, the user's public key.

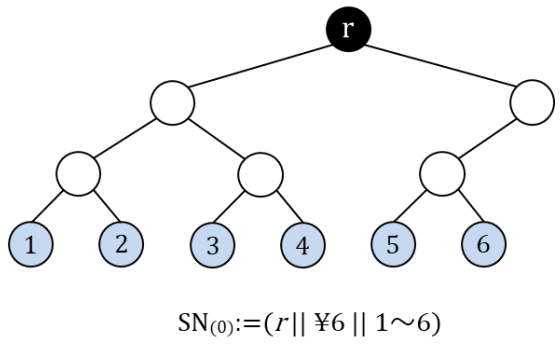


Figure 8: Method for generating serial numbers for electronic cash in the variable denomination scheme (Example of constructing 6 yen using a binary tree)

(ii) Transmission of electronic cash

A process where user U sends 4 yen of the 6 yen electronic cash issued by the service provider, to user V is as follows[51]:

(1) User U reconstructs the binary tree indicated by the serial number $\mathrm{SN}_{(0)}$ of $T_{(0)}$ and assigns r_0 to the root of the subtree representing the 4 yen to be sent (leaves labeled 1–4) by calculating $r_0||r_1 \leftarrow G(r)$[52], where G is a common function that generates $2m$-bit pseudo-random numbers from an m-bit input.

[51] When sending an amount such as 5 yen out of 6 yen, the tree composed of the leaves corresponding to the amount to be sent becomes the entire tree. In such cases, pseudo-random numbers generated by G are unnecessary, and the first element of the serial number generated in Step 2 will be the root value r, of the tree.

[52] r_1 generated by $G(r)$ is used to send partial trees with leaves labeled 5 to 6.

(2) User U generates a new serial number $\mathrm{SN}_{(1,1)} \leftarrow (r_0 \,||\, ¥4 \,||\, 1{\sim}4)$ for the sent electronic cash. Here, $\mathrm{SN}_{(n,k)}$ denotes the serial number assigned to the k-th electronic cash generated by splitting $T_{(n-1,x)}$ $(x \geq k)$ (see Figure 9). To update the electronic cash and transfer record, user U generates $T_{(1,1)} \leftarrow \mathrm{Sign}_{\mathrm{sk}_U}(T_{(0)} \,\|\, \mathrm{SN}_{(1,1)} \,\|\, ¥4)$ and $\sigma_{(1,1)} \leftarrow \mathrm{Sign}_{\mathrm{sk}_U}(\sigma_{(0)} \,\|\, \mathrm{SN}_{(1,1)} \,\|\, ¥4 \,\|\, \mathrm{pk}_V)$ for the recipient's public key pk_V, and sends $(\mathrm{SN}_{(1,1)}, T_{(1,1)}, \sigma_{(1,1)}, \mathrm{SN}_{(0)}, T_{(0)}, \sigma_{(0)})$ along with public key pk_U and its certificate to user V. The message part of the signatures by the users includes the pre-split electronic cash $T_{(0)}$ and transfer record $\sigma_{(0)}$ respectively, creating a linked signature chain. Measures such as one-time identifiers or challenge-response methods are employed to prevent duplication of electronic cash for the same user.

(3) User U saves the unused portion of $T_{(0)}$ (labels 5–6) along with $(T_{(0)}, \sigma_{(0)})$ on their device.

- For subsequent transfers of the remaining 2 yen or any part of it, user U follows the same procedure as in Step 2 to create the corresponding electronic cash and transfer record based on $(T_{(0)}, \sigma_{(0)})$.

(4) User V verifies the validity of the received $(\mathrm{SN}_{(1,1)}, T_{(1,1)}, \sigma_{(1,1)}, \mathrm{SN}_{(0)}, T_{(0)}, \sigma_{(0)})$ by checking the following:

- $\mathrm{SN}_{(1,1)}$ is correctly generated:
  - For $r \in \mathrm{SN}_{(0)}$, $x \leftarrow G(r)$ ensures the upper m bits of x are elements of $\mathrm{SN}_{(1,1)}$,
- $T_{(1,1)}$ and $\sigma_{(1,1)}$ are correctly generated:
  - Both are signed by the sender U,
  - $\sigma_{(1,1)}$ includes a signature on the recipient's public key pk_V,
- $T_{(0)}$ and $\sigma_{(0)}$ are correctlygenerated:
  - Both are signatures by the service provider on the same serial number $(\mathrm{SN}_{(0)})$;
- $\sigma_{(0)}$'s message contains the public key pk_U, of the signer of $\sigma_{(1,1)}$.

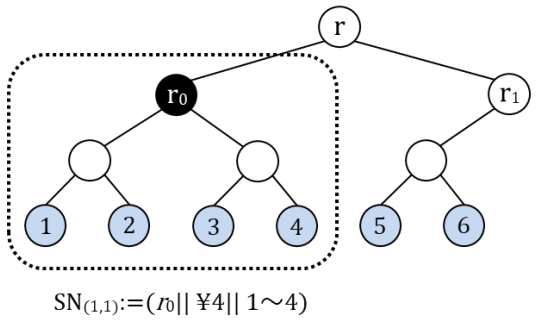


Figure 9: Method for splitting electronic cash in the variable denomination scheme (Splitting and sending 4 yen out of 6 yen)

(4) Electronic cash scheme with enhanced privacy

As summarized in Chapter 2, to achieve unlinkability in electronic cash scheme, it is necessary to change the public key each time electronic cash is sent or received. However, frequent updates to public keys would significantly increase the certificate issuance and management costs on the part of the certification authority, while also leading to processing delays and reduced usability. This section considers a method to enhance user privacy without increasing the certificate issuance and management costs for the certification authority[53]. However, since this method utilizes zero-knowledge proofs, the processing and communication costs for sending and receiving electronic cash become relatively higher. It should be noted that the implementation of this method requires improvements in the performance of user devices and communication speed.

The following three requirements must be addressed from a privacy protection standpoint when implementing the enhanced privacy electronic cash scheme:

Requirement (1) Unlinkability of electronic cash transactions carried out by the same user:

- If the same public key is included in the transfer record of multiple items of electronic cash, information related to the user corresponding to that public key (e.g., purchasing history) could be leaked.

Requirement (2) Verifiability of legitimate transactions even under anonymity and unlinkability: Even when anonymity and unlinkability are ensured, the recipient of the electronic cash must be able to confirm that the transaction was conducted by a legitimate user registered with the certification authority.

- Traditionally, this confirmation was achieved by verifying the certificate issued by the certification authority. The enhanced privacy scheme must also meet this requirement.

Requirement (3) Identification of users engaging in double spending: Even when anonymity and unlinkability are ensured, the service provider must be able to identify users who engage in double spending.

[53] Since the method discussed in this chapter does not support the variable denomination scheme described in section (3) of this chapter, it is necessary to consider the enhancement of the privacy of the variable denomination scheme separately.

- Similar to conventional electronic cash systems, the ability to identify fraudulent users is essential.

To enhance privacy, the proposed scheme introduces a transaction-specific public key in addition to the public key registered with the certification authority. By allowing users to update their transaction-specific public key for each transaction, the scheme protects user privacy from service providers and other users (Requirement (1)). Furthermore, the transaction-specific public key is associated with the certificate issued by the certification authority, and their relationship is verified to confirm that the user is conducting transactions with a valid key registered with the certification authority (Requirement (2)). Additionally, as with the basic electronic cash scheme in chapter 2, this enhanced privacy scheme leverages the properties of zero-knowledge proofs to identify users from double spent electronic cash (Requirement (3)).

In this scheme, the sender and recipient of electronic cash execute a non-interactive protocol based on the Σ protocol, a type of zero-knowledge proof (see Appendix 3 (1)). The Σ protocol allows the prover to demonstrate to the verifier that certain secret information satisfies a specific condition without revealing the information itself. In this scheme, the Σ protocol is used to satisfy Requirement (2), wherein the sender of the electronic cash acts as the prover, and the recipient acts as the verifier.

In the non-interactive setting, the prover generates and transmits three types of data to the verifier: commitment, challenge, and response. A notable property of the Σ protocol is that if two different challenges and responses exist for the same commitment, the prover's secret information is exposed. The proposed scheme uses this property to identify users who double spend the electronic cash. Specifically, the commitment generated by the user is embedded in the digital signature (transfer record of the electronic cash) in a tamper-proof format. As a result, even in cases of double spending, the commitment remains identical. To achieve this, the commitment is generated when the electronic cash is received, not when it is sent. As in the basic electronic cash system in chapter 2, the electronic cash T and its transfer record σ are transmitted and received as a set in this scheme.

The requirements (1)-(3) mentioned above are fulfilled through the following methods:

- Generation and update of transaction-specific public key $\mathrm{pk}_{(i)}$: Users generate their own transaction-specific public keys and update them for each i-th transaction.

- Certificate issuance and self-signing: Users obtain a certificate Cer for their pubic key pk from the certification authority and generate a self-signed certificate $\mathrm{Cer}_{(i)}$ for the transaction-specific public key $\mathrm{pk}_{(i)}$ using their private key sk. By proving that Cer and $\mathrm{Cer}_{(i)}$ correspond to the same public key, it can be verified that the transaction through $\mathrm{pk}_{(i)}$ was conducted by a legitimate user registered with the service provider. Additionally, anonymity against the service provider is ensured by using zero-knowledge proofs to conceal the public key pk and certificate Cer.
- Identification of fraudulent users: The service provider leverages the properties of zero-knowledge proofs to identify the public key pk of users who engage in double spending.

The specific procedures are summarized in (i)-(iv) (Figure 10). For details of the protocol, refer to the Appendix 3 (2) (iii).

In this method, unless double spending occurs, the user's public key is not disclosed to the service provider[54]. Therefore, from the perspective of AML/CFT, a potential approach might involve intentionally simulating double spending for high-value transactions on the application level, allowing the service provider to identify the user (Otsuka [2022]).

(i) Initial setup

The certification authority and users prepare the key pairs and the certificates as follows:

(1) The certification authority generates a pair of private and public keys $(\mathrm{sk}_C, \mathrm{pk}_C)$ and publishes them along with its self-signed certificate.

(2) User U generates a key pair $(\mathrm{sk}_U, \mathrm{pk}_U)$ and sends pk_U to the certification authority.

(3) The certification authority issues a certificate Cer_U for the public key pk_U and provides it to user U.

(ii) Receipt of electronic cash

A process user U receives electronic cash T from user V is as follows:

(1) User U randomly generates a transaction-specific public key $\mathrm{pk}_{U(i)}$, where i is the transaction ID for U.

(2) User U creates a self-signed certificate $\mathrm{Cer}_{U(i)}$ for $\mathrm{pk}_{U(i)}$ using sk_U.

[54] In this method, even service providers find it difficult to determine the user's public key from the transfer record of redeemed electronic cash. Therefore, even if the service provider, rather than the certification authority, handles user registration and manages user information, it is still possible to satisfy the anonymity and unlinkability of electronic cash.

- Public key $\mathrm{pk}_{U(i)}$ is generated specifically for the transaction involving the electronic cash received from user V.

(3) User U sends the transaction-specific public key $\mathrm{pk}_{U(i)}$ to be used for electronic cash T and commitment $\mathrm{com}_{(i)}$ to user V upon the latter's request[55].

- $\mathrm{com}_{(i)}$, generated by user U, is intended for use in the Σ protocol[56] when the electronic cash is later sent to user W. However, it is generated at this stage and sent to user V to enable identification of double-spending users.

(4) User U receives the electronic cash T, its transfer record $\{\sigma_{(\ell)}\}_{0\leq\ell\leq n}$, and the transaction-specific public keys of previous users included in the transfer record, from user V.

- $\sigma_{(n)}$ consists of the commitment $\mathrm{com}_{(k)}$ and response $\mathrm{res}_{(k)}$ from user V under the Σ-protocol[57]. Here, n represents the number of times the electronic cash T has been transferred.

(5) User U verifies the validity of T and $\{\sigma_{(\ell)}\}_{0\leq\ell\leq n}$. If the verification is successful, user U accepts the electronic cash; otherwise, rejects it. When transferring m items of electronic cash, this process is repeated m times.

(iii) Transmission of electronic cash

A process user U sends the electronic cash T received from user V to user W is as follows:

(1) User U requests the transaction-specific public key $\mathrm{pk}_{W(j)}$ and commitment $\mathrm{com}_{(j)}$ from user W, where j is the transaction ID for user W.

(2) User U discloses $\mathrm{pk}_{U(i)}$ and generates a challenge $\mathrm{chal}_{(i)}$ and a response $\mathrm{res}_{(i)}$. Using the previously generated $\mathrm{com}_{(i)}$, along with $(\mathrm{chal}_{(i)}, \mathrm{res}_{(i)})$, user U proves that they are a legitimate user registered with the certification authority (i.e., they possess the private key corresponding to the public key registered with the certification authority). While $\mathrm{pk}_{U(i)}$ is disclosed, neither the self-signed certificate $\mathrm{Cer}_{U(i)}$, the public key pk_U, nor the certificate Cer_U are revealed. User U demonstrates that:

- they possess the self-signed certificate $\mathrm{Cer}_{U(i)}$ corresponding to $\mathrm{pk}_{U(i)}$ and the public key pk_U corresponding to the private key used to generate $\mathrm{Cer}_{U(i)}$,
- they possess the certificate Cer_U issued for the above public key pk_U, and
- that $(\mathrm{pk}_{W(j)}, \mathrm{com}_{(j)}, \mathrm{com}_{(i)}, T)$ have not been tampered with.

---

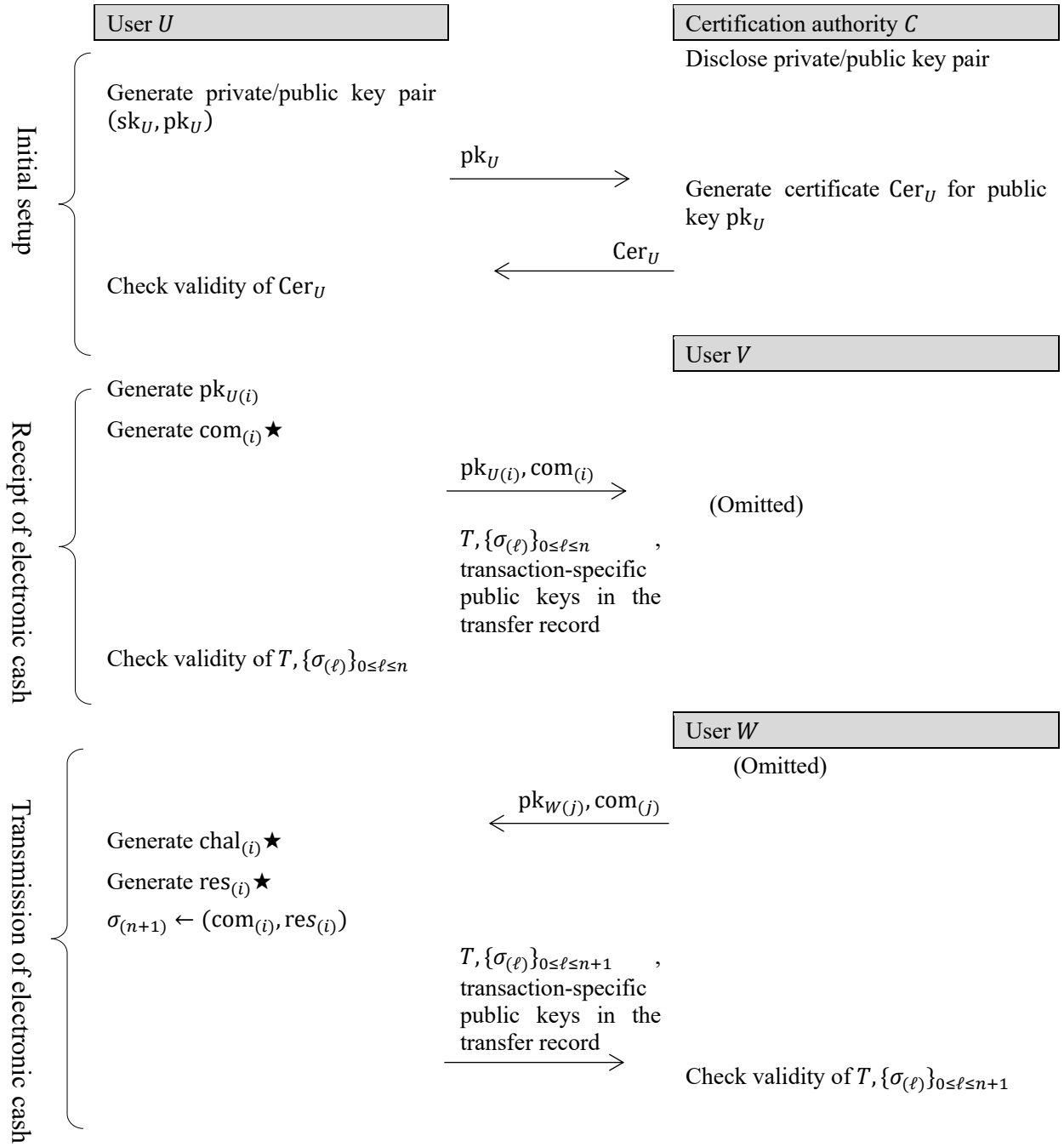
[55] A commitment to x refers to data generated in such a way that when user U sends the commitment to user V, it is difficult for user V to determine the value of x from the commitment, and user U cannot alter the value of x after sending the commitment. Additionally, the function used to compute the commitment is referred to as a commitment function.

[56] Σ protocol in which the prover is user U and the verifier is user W.

[57] Σ protocol in which the prover is user V and the verifier is user U.

(3) User U generates $\sigma_{(n+1)} = (\mathrm{com}_{(i)}, \mathrm{res}_{(i)})$ and sends $(T, \{\sigma_{(\ell)}\}_{0 \le \ell \le n+1})$, along with the transaction-specific public keys of previous users in the transfer record, to user W.

(4) User W verifies the validity of T and $\{\sigma_{(\ell)}\}_{0 \le \ell \le n+1}$. If the verification is successful, user W accepts the electronic cash; otherwise, rejects it. This process is repeated m times when receiving m items of electronic cash.



Note: ★ refers to the commitment, challenge, and response used in the Σ protocol that user U executes when sending to user V.

Figure 10: Privacy-enhanced electronic cash transmission and reception protocol

(iv)Detection of double spending

The service provider determines that electronic cash is double spent if its serial number is not found in the Issued Electronic Cash DB. Leveraging the properties of the Σ protocol, the service provider can identify the public key of the user who engaged in double spending and verify the corresponding user with the certification authority.

5. Conclusion

In this paper, we focused on electronic cash system, a payment system that does not rely on a ledger and revisited its characteristics while conducting practical verification based on widely used contemporary devices. During the experimental trials of the 1990s, the usability of electronic cash system was likely limited due to significant constraints on the performance of IC cards and communication environments at the time. In contrast, the present verification, conducted with the assumption of smartphone usage, demonstrated that, in theory, transactions involving the transfer of 100 items of electronic cash could be processed in approximately the same amount of time as existing contactless IC card payment systems. However, it should be noted that this verification measured only transaction response times; in practice, additional time for application operations and establishing smartphone connections must also be taken into account. This evaluation was limited to the processes of sending and receiving electronic cash items, leaving numerous issues for further consideration. For instance, in this study, we assumed the presence of an independent institution responsible for user identity verification and certificate issuance to enhance privacy protection from service providers. However, to achieve practical implementation, a review of compliance with existing laws will also be required. Additionally, while this paper focused on the retrospective traceability of electronic cash items for AML/CFT purposes, further studies are necessary to explore other potential methods of compliance.

As part of our future-oriented discussions, we also considered a scheme enabling the division and aggregation of electronic cash items into arbitrary amounts. Such a scheme would eliminate the need for transactions involving change or currency exchange, thereby improving usability. Moreover, the proposed scheme, which treats electronic cash items for each unit amount independently, differs from methods that merely aggregate monetary values during

division or aggregation. It enables tracing of doubly spent electronic cash items even if mixed with other items. Detailed evaluations of the security of this variable denomination scheme and practical verification on actual devices are planned going forward.

We also explored a protocol designed to enhance privacy. This protocol ensures that even service providers cannot easily obtain information about users' transactions from redeemed electronic cash items. However, processing with zero-knowledge proofs incurs higher computational costs and larger signature sizes compared to conventional digital signatures. Thus, improved device performance and communication speeds are prerequisites for its implementation. At present, this aspect remains a theoretical exploration, but it is expected to be valuable for future discussions.

The rapid advancement of information and communication technology is likely to continue reshaping our devices, network structures, and lifestyles. Moving forward, we aim to continue evaluating the feasibility of electronic cash system through practical verification while also exploring new possibilities in anticipation of future technological advancements. We hope that the results of this study will contribute to the realization of more efficient and user-friendly payment services.

References

Bernstein, Daniel J., Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang, “High-Speed High-Security Signatures,” Journal of Cryptographic Engineering, 2012, pp. 77–89.

Certicom Research, “SEC 1: Elliptic Curve Cryptography (Version 1.0),” The Standards for Efficient Cryptography Group, 2000 (available at https://www.secg.org/SEC1-Ver-1.0.pdf, accessed November 1 2024).

Chaum, David, “Blind Signatures for Untraceable Payments,” Proceedings of CRYPTO ’82, Lecture Notes in Computer Science, 1440, Springer, 1983, pp. 199–203.

Consumption and Distribution Policy Division, Commerce and Service Group, Ministry of Economy, Trade and Industry, "Cashless Vision," Ministry of Economy, Trade and Industry, 2018 (available at http://www.meti.go.jp/policy/mono_info_service/cashless/image_PDF_ movie/cl_vision.pdf, accessed November 1 2024, in Japanese).

Cyber Business Council, “Internet Cash Verification Report,” E-Japan Council, 2000 (in Japanese).

Financial Research Study Group, "Development of a Cashless Society and the Role of the Financial System," Japanese Bankers Association, 2018 (available at https://www.zenginkyo.or.jp/fileadmin/res/news/news300437_1.pdf, accessed November 1 2024).

Fujisaki, Eiichiro, "Study and Evaluation of the Security of the Digital Signature EdDSA Configuration," 2020 Cryptographic Research Report, CRYPTREC, 2020 (available at https://www.cryptrec.go.jp/exreport/cryptrec-ex-3002-2020.pdf, accessed November 1 2024, in Japanese).

Furuichi, Mineko, "Legal Discussion on Cash and Money," Monetary and Economic Studies, Vol.14, No.4, Institute for Monetary and Economic Studies, Bank of Japan, pp. 101–152, 1995 (in Japanese).

Hojo, Masashi, and Junichiro Hatogai, "Programmability of Payment and Settlement Systems," Bank of Japan Review, No. 2022-E-12, Bank of Japan, 2022 (in Japanese).

Isobe, Kohei, and Masashi Une, "Security in Smartphones and Other Smart Devices: The Current State and Prospects of Risks Associated with Platforms," Monetary and Economic Studies, Vol. 40, No. 3, Institute for Monetary and Economic Studies, Bank of Japan, 2021, pp. 77–102 (in Japanese).

Ministry of Economy, Trade and Industry, "Cashless Payment Ratio Calculated for 2023 - 39.3%, Cashless Payment Ratio Expanding Steadily Toward 2025," 2024 (available at https://www.meti.go.jp/press/2023/03/20240329006/20240329006.html, accessed November 1 2024, in Japanese).

Nakata, Masao, "Issues to be Examined in Conjunction with the Advancement of Cashless Face-to-Face Payments and the Directions for their Support," Journal of Research on Social and Economic Life, Vol. 61, No. 2, pp. 32–55, 2021 (in Japanese).

Nakayama, Yasushi, Hidemi Moribatake, Masayuki Abe, and Eiichiro Fujisaki, "A Method of Realizing Electronic Money: A Proposal of a New method of Realizing Electronic Money that Takes into Consideration Safety and Convenience," Monetary and Economic Studies, Vol.16, No.2, Institute for Monetary and Economic Studies, Bank of Japan, pp. 75–86, 1997 (in Japanese).

Nielsen, Jakob, “Website Response Times,” Nielsen Norman Group, 2010 (available at https://www.nngroup.com/articles/website-response-times/, accessed November 1 2024).

Noda, Kohei, "Recirculation of Underground Funds: The Fight Against Crime, Terrorism, and Nuclear Development Money: Chapter 12: Digital Revolution and Underground Funds," The Finance, 2022 July Edition, Ministry of Finance, 2022, pp. 40–50 (in Japanese).

NTT, “Development of Experimental System for an Electronic Cash System Using Cryptography to Enable Privacy Protection of Users and High Level of Safety,” NTT NEWS RELEASE, NTT, 1995 (in Japanese).

-------, "Prototype of a New Electronic Money System: Adopting a New System with Higher Level of Safety, Reliability and Efficiency", NTT NEWS RELEASE, NTT, 1996 (in Japanese).

NTT Communications Corporation, "Future Initiatives of NTT Communications Regarding the Electronic Money ‘Super Cash’," 2000 (in Japanese).

NTT DoCoMo Mobile Society Research Institute, "2024 Smartphone Use Ratio 97%: About 4% in 2010," NTT DoCoMo Mobile Society Research Institute, 2024 (available at https://www.moba- ken.jp/project/mobile/20240415.html, accessed November 1 2024, in Japanese).

NTT Network Service Systems Laboratories, “Inclusive Core: Integrative and Cooperative Network Architecture for the 6G/IOWN Era” - White Paper, NTT, 2023 (available at https://www.rd.nt/ns/incluivecore/whitepaper_ver1.html, accessed November 1 2024, in Japanese).

Okamoto, Tatsuaki, and Kazuo Ohta, “Universal Electronic Cash,” Advances in Cryptology - Proceedings of CRYPTO’91, Lecture Notes in Computer Science, 576, Springer, 1992, pp. 324–337.

Okamoto, Tatsuaki, and Kazuo Ohta, "An Ideal Method for the Electronic Cash System," IEICE Transactions, Vol. J76-D-I, No. 6, pp. 315–323, 1993 (in Japanese).

Ootsuki, Satoshi, “Outline of the Suica System,” J. IEIE Jpn. Vol. 31, No. 6, pp. 408–411, 2011 (in Japanese).

Otsuka, Akira, "Research Trends in Tamper-Resistant Digital Currency Wallets: Balancing Anonymity and Transparency," IMES Discussion Paper No. 2022-J-9, Institute for Monetary and Economic Studies, Bank of Japan, 2022 (in Japanese).

Soyama, Tomoyuki, "Suica Data and Services: Hybrid Online and Offline," Future Forum on Payment and Settlement, Digital Currency Subcommittee: Lecture on Digital Payments in the Post-Covid19 Era, Payment and Settlement Systems Department, Bank of Japan, 2020 (available at https://www.boj.or.jp/paym/outline/mirai_forum/data/rel200911b8.pdf, accessed November 1 2024, in Japaese).

Takahashi, Kenta, "Biometric Authentication Infrastructure in the Era of Digital Trust: Public Biometric Infrastructure (PBI) and Related Technologies," Lecture Material at the 22nd Information Security Symposium, Institute for Monetary and Economic Studies, Bank of Japan, 2021 (in Japanese).

Tamura, Yuko, and Masashi Une, "Security Countermeasures for IC Card-based Identity System and Issues to Consider", Monetary and Economic Studies, Vol. 26, Vol.1, Institute for Monetary and Economic Studies, Bank of Japan, pp. 53–100, 2007 (in Japanese).

Une, Masashi, "How to Cope with the Impact of Quantum Computers on Cryptography: Overseas Initiatives," IMES Discussion Paper, No. 2023-J-13, Institute for Monetary and Economic Studies, Bank of Japan, 2023 (in Japanese).

Visa, “Contactless Payments,” VISA Canada, 2014 (available at https://www.visa.ca.dam/VCOM/regional/na/canada/merchants/documents/visa-paywave-put-your-customer-in-the-fast-lane-en.pdf, accessed November 1 2024).

Appendix 1. Certificate issuance procedure when the functions of the certification authority are divided

This section outlines the procedure for user registration and certificate issuance when the tasks of managing user information and issuing certificates are handled separately, as discussed in Chapter 2 (3) (see Figure A-1). Here, the entity managing the user information is referred to as the Registration Authority (RA), the entity issuing and managing certificates is referred to as the Issuing Authority (IA), and the combined entities are collectively referred to as the Certification Authority (CA).

(1) The user applies for the service via an application installed in the normal domain of their device (hereafter referred to as the normal domain app) and sends a certificate issuance request to the RA. At this stage, the RA requests the user's device identifier information[58] from the device.

(2) The RA reviews the contents of the submitted application form[59]. If necessary, the RA conducts identity verification.

(3) If the RA finds no issues in the review, it issues a user identification code to the normal domain app and links it to the user information submitted by the user.

(4) The RA sends a notification of the completed review and the user identification code to the normal domain app.

(5) Upon receiving the review completion notification, the normal domain app instructs the application installed in the secure domain (hereafter referred to as the secure domain app) to generate a key pair and create a Certificate Signing Request (CSR).

(6) The secure domain app generates the key pair and the CSR.

(7) The secure domain app links the CSR generated within the secure domain to the normal domain app.

(8) The normal domain app sends the CSR, the user identification code, and the device identifier information to the IA, requesting the issuance of a certificate.

(9) The IA verifies that there are no issues with the received CSR and user identification code (e.g., no duplication) and generates the certificate.

(10) The secure domain app performs an integrity check on the public key and stores the certificate in the secure domain.

[58] Information that can be used as device identifier information includes the International Mobile Equipment Identity (IMEI) and IDs assigned to each device's eSE. The choice should be made based on the security and usability requirements of the service.

[59] An assessment is conducted to ensure there are no issues with allowing the user to access the service. For example, this may involve verifying that the user has not previously violated the terms of service.

(11) The secure domain app generates a receipt notification within the secure domain and sends it to the IA via the normal domain app.

(12) The IA confirms the receipt notification.

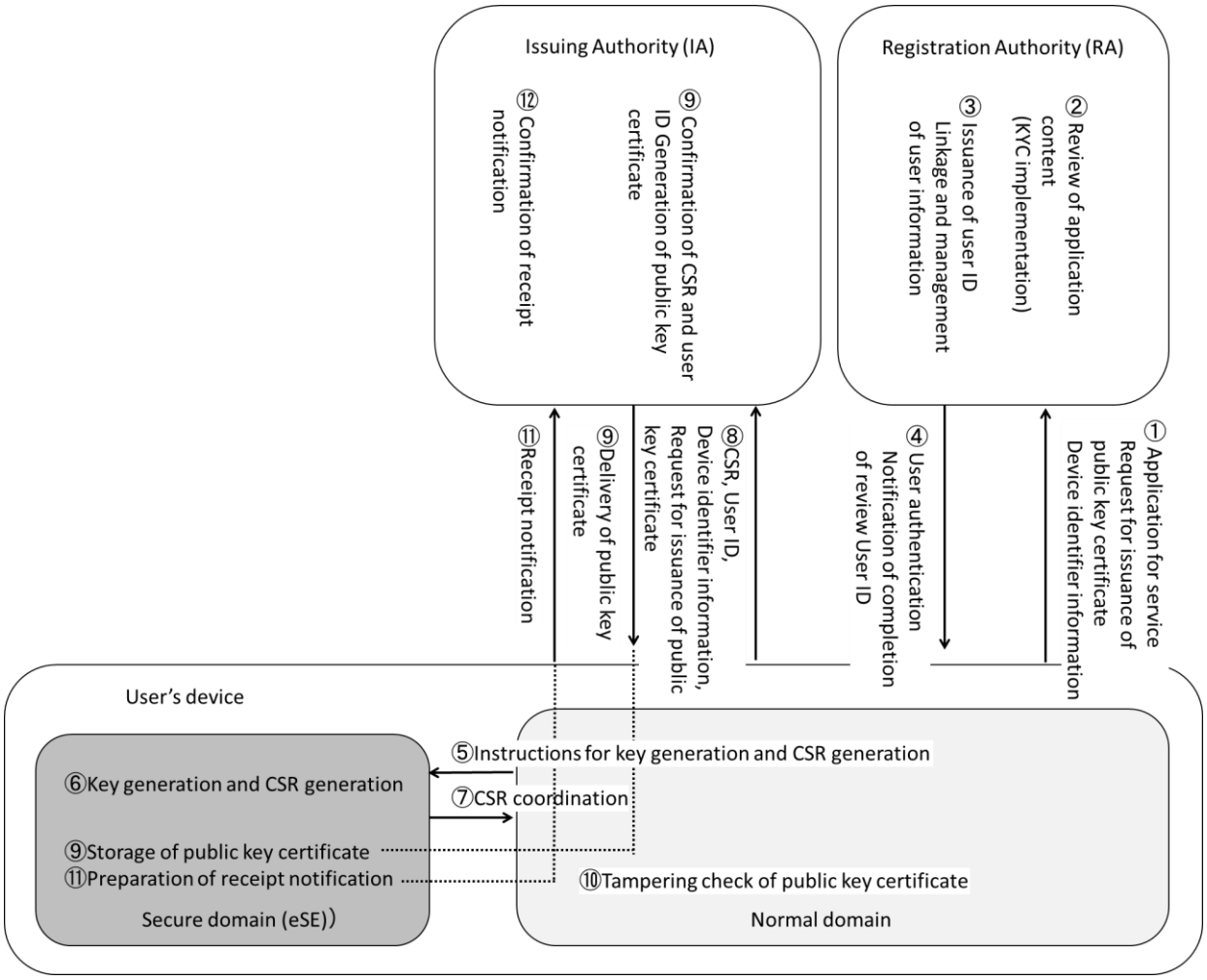


Figure A-1: Certificate issuance procedure when the functions of the certification authority are divided

Appendix 2: Optimization of electronic cash systems

(1) Enhancing the efficiency of electronic cash transmission and receipt

This section elaborates on the detailed protocol for optimizing the transmission and receipt of electronic cash as outlined in chapter 4 (1).

(a) Initial setup (Three algorithms)

The method using a Merkle tree (Figure A-2) employs the following three algorithms: MHTree, MHPath, and MHVer.

- $(L, h) \leftarrow \mathrm{MHTree}(D)$
  - The function MHTree takes a dataset D as input and outputs a Merkle tree L, with the elements of D $(= \{(i, h_i)\})$ as leaf nodes, and the root value h. A Merkle tree is a tree structure generated by repeatedly assigning the hash values of two child nodes to their parent node. Here, i is the node identifier, and h_i denotes the value labeled on the node. For example, the identifiers of the leaf nodes at depth 3 are represented by 3-digit binary numbers, sequentially numbered as 000, 001, ..., 111. If the number of elements in D is insufficient for constructing a full binary tree, the algorithm outputs a Merkle tree where the remaining nodes are labeled with $h_i = \text{"}00\cdots\text{"}$. Using a hash function H, the tree assigns $H(h_{000}, h_{001})$ to h_{00}, $H(h_{00}, h_{01})$ to h_0, and so forth. Figure A-2 illustrates a tree where the value of the node identified by i is represented as h_i.
- $(AP, h) \leftarrow \mathrm{MHPath}(D, D')$
  - The MHPath function takes a dataset D and its subset $D'(\subset D)$ as inputs and outputs the path AP required to calculate from D' the root h of the Merkle tree generated from D, as well as the root value h.
  - For example, if $D' = \{(000, h_{000}), (100, h_{100}), (101, h_{101})\}$, the algorithm outputs $\mathrm{AP} = \{(001, h_{001}), (01, h_{01}), (11, h_{11})\}$ and h for the input of D' (see Figure A-3).
- $1/0 \leftarrow \mathrm{MHVer}(D', AP, h)$
  - The MHVer function takes a dataset D', a path AP, and a root value h as inputs. It verifies whether the root value of the Merkle tree with $D' \cup \mathrm{AP}$ as the node matches h. The function returns 1 if they match and 0 otherwise.

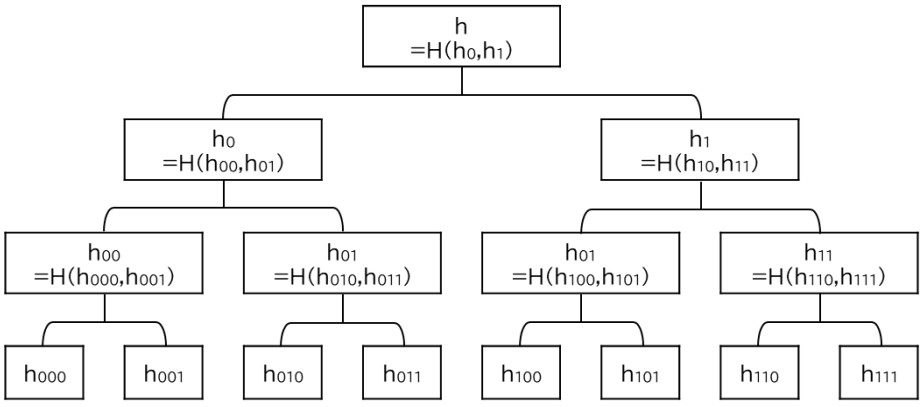


Figure A-2: Structure of Merkle trees

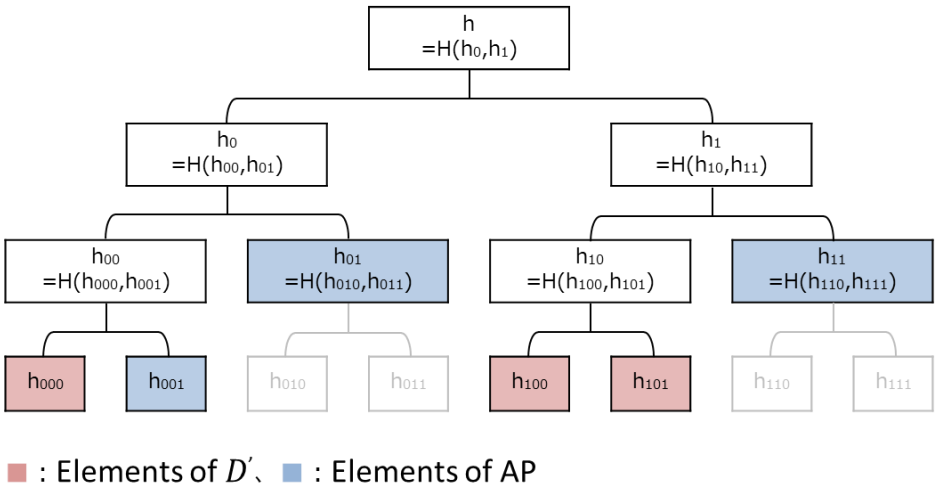


Figure A-3: Relationship between input (D') and output (AP) of the MHPath function

(b) Processing of electronic cash transmission and receipt

The specific steps for user U to transfer electronic cash to user V are as follows:

1. User U requests and verifies the certificate Cer_V from the recipient user V.
2. User U calculates $h_i \leftarrow H(\sigma_{i(n_i)})(1 \le i \le m)$ for the m electronic cash $T_i(1 \le i \le m)$ being transmitted and their respective transfer records $\sigma_{i(\ell)}(1 \le i \le m, 0 \le \ell \le n_i)$. Here, n_i denotes the number of transfers for T_i and $\sigma_{i(\ell)}$ represents the transfer record at the ℓ-th transfer. $\sigma_{i(0)}$ is the initial transfer record assigned at issuance of T_i. The Merkle tree L with $\{h_i\}_{1 \le i \le m}$ as leaf nodes and root value h are computed using $(L, h) \leftarrow \mathrm{MHTree}(\{(i, h_i)\}_{1 \le i \le m})$.
3. User U updates the transfer record by generating a digital signature $\sigma \leftarrow \mathrm{Sign}_{\mathrm{sk}_U}(h \parallel \mathrm{pk}_V)$ for root h and pk_V, the public key of user V.
4. User U sends their certificate Cer_U, the m electronic cash, and their transfer records to user V. The transmitted data include $(\{T_i\}_{1 \le i \le m}, \sigma, \{\sigma_{i(\ell)}\}_{1 \le i \le m, 0 \le \ell \le n_i})$, along with $(\mathrm{AP}_j, h_j) \leftarrow \mathrm{MHPath}(\{\sigma_j\}, \sigma_{i(n_i-1)})$, which is necessary to verify previous transfer records $\sigma_{i(\ell)}(0 \le \ell \le n_i)$. Here, $\{\sigma_j\}$ represents the transfer record of electronic cash $\{T_j\}(\ni T_i)$ sent upon receiving electronic cash T_i from user U_j in the the past.
   - The updated transfer record σ is common across the m items of electronic cash T_i and represented as $\sigma = \sigma_{1(n_1)} = \sigma_{2(n_2)} = \cdots = \sigma_{m(n_m)}$.
5. User V verifies the validity of Cer_U, confirms that the received electronic cash was correctly transmitted, and saves it to their device.

- This involves calculating $(L, h) \leftarrow \mathrm{MHTree}(\{(i, \sigma_{i(n_i)})\}_{1 \le i \le m})$ and verifying that σ is a valid signature for h by user U.
- Using $\mathrm{MHVer}(\sigma_{i(n_i)}, \mathrm{AP}_j, h_j)$, user V verifies the validity of h_j and confirms that $\sigma_{i(n_i)}$ is a valid signature for h_j. This process is repeated for all transfer records $\sigma_{i(\ell)} (1 \le i \le m, 0 \le \ell \le n_i)$.

(2) Enhancing the efficiency of electronic cash redemption

EdDSA consists of three algorithms (key generation, signature generation, and signature verification) under the following parameter settings (Bernstein *et al*. [2012], Fujisaki [2020]).

Parameter settings:

The parameters used in EdDSA are as follows:

- Odd prime number q, finite field $\mathbb{F}_q$
- Positive integer b: the length of the public key. Note that $q < 2^{b-1}$.
- Hash function $H: \{0,1\}^* \to \{0,1\}^{2b}$
- Encoding function: $\mathbb{F}_q \to \{0,1\}^{b-1}$ (converts elements of $\mathbb{F}_q$ into $(b-1)$ bit representation).
- (Twisted) Edwards curve over $\mathbb{F}_q$:

  $E(\mathbb{F}_q): \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : ax^2 + y^2 = 1 + dx^2y^2\}$.

  a: quadratic residue over $\mathbb{F}_q$, d: (non-zero) quadratic non-residue over $\mathbb{F}_q$.

  If $q \equiv 1 \ (mod\ 4)$, then $a = -1$; if $q \equiv 3 \ (mod\ 4)$, then $a = 1$.

  The order of E, denoted $\#E = 2^c * l$, where $c = 2\ or\ 3$, and 2^c is called the cofactor.
- Base point $B \in E$, $B \neq (0,1)$, $lB = (0,1)$, where l is a prime number. The cyclic group generated by B has order $\#B = l$.

When the addition on the Edwards curve is defined as follows, E becomes an additive group with the identity element $O = (0,1)$:

$$(\boldsymbol{x_1}, \boldsymbol{y_1}) + (\boldsymbol{x_2}, \boldsymbol{y_2}) \coloneqq \left(\frac{(\boldsymbol{x_1 y_2} + \boldsymbol{x_2 y_1})}{\boldsymbol{1} + \boldsymbol{d x_1 x_2 y_1 y_2}}, \frac{(\boldsymbol{y_1 y_2} + \boldsymbol{x_1 x_2})}{\boldsymbol{1} - \boldsymbol{d x_1 x_2 y_1 y_2}} \right)$$

Key generation:

A user generates the private key k and public key A as follows:

- $k \leftarrow \{0,1\}^b$
- $(h_0, h_1, \dots, h_{2b-1}) \leftarrow H(k)$
- $a \leftarrow 2^{2b-2} + \sum_{3 \le i \le b-3} 2^i h_i \in \{2^{2b-2}, 2^{2b-2} + 8, \dots, 2^{2b-1} - 8\}$
- $A \leftarrow aB$

Private key: k

Public key: $\underline{A} := aB$ (where $\underline{A}$ is the encoded value of A)

Signature generation:

The signer uses $(h_b, \dots, h_{2b-1})(= H(k))$ (derived from k) to generate the signature $(\underline{R}, \underline{S})$ for message M as follows:

- $r \leftarrow H(h_b, \dots, h_{2b-1}, M) \in \{0,1, \dots, 2^{2b} - 1\}$.
- $R \leftarrow rB$.
- $S \leftarrow \left(r + H\left(\underline{R}, \underline{A}, M\right)a\right) \bmod l$.

Signature verification:

The verifier uses the public key $\underline{A}$ of the signer to confirm the validity of the signature $(\underline{R}, \underline{S})$ for message M by checking the following equation:

- $2^c SB = 2^c R + 2^c H(\underline{R}, \underline{A}, M)A$.

Batch verification:

For multiple signatures $(\underline{R_i}, \underline{S_i})$ corresponding to messages M_i by public keys A_i, batch verification can be performed by linearly combining the signature verification equations as follows:

- Select random integers z_i based on the parameters and the number of signatures and compute $H_i = H(R_i, A_i, M_i)$.
- Confirm the validity of the following equation:

$$(-\Sigma_i z_i S_i \; mod \; l)B + \Sigma_i z_i R_i + \Sigma_i (z_i H_i mod \; l)A_i = 0$$

Appendix 3: Privacy-enhanced electronic cash protocol

Here, in addition to the protocol proposed in Chapter 4 (4), two alternative methods are introduced: (1) a method where the user's private key is registered with the service provider, and malicious actors are identified using the user's private information, and (2) a method where only the user's public key is registered with the service provider, and malicious actors are identified using the user's private information. Compared to the method introduced in Chapter 4, these approaches are less secure in terms of operational safety but offer the advantage of lower computational costs.

(1) Σ Protocol

The Σ protocol is a zero-knowledge proof protocol that demonstrates knowledge of a witness w for x, which belongs to the language $L_R = \{x \mid \exists w, (x, w) \in R\}$ (proof that x belongs to language L), by exchanging the data called "commitment," "challenge," and "response" between the prover and the verifier.

The prover first sends a commitment com to the verifier, which is generated using public information x, the witness w, and a random number r. The verifier then sends a challenge chal, generated using a sufficiently secure random number generation function, to the prover. Finally, the prover sends a response res to the verifier. If the prover knows the witness w for x, it can generate res using a function RES such that $1 \leftarrow \mathrm{VER}(\mathrm{com}, \mathrm{chal}, \mathrm{res}, x)$ in response to the exchanged com and chal. For a user who does not know w, the probability of generating res that satisfies $1 \leftarrow \mathrm{VER}(\mathrm{com}, \mathrm{chal}, \mathrm{res}, x)$ is negligibly small, and with overwhelming probability, becomes $0 \leftarrow \mathrm{VER}(\mathrm{com}, \mathrm{chal}, \mathrm{res}, x)$ (refer to Figure A-4).

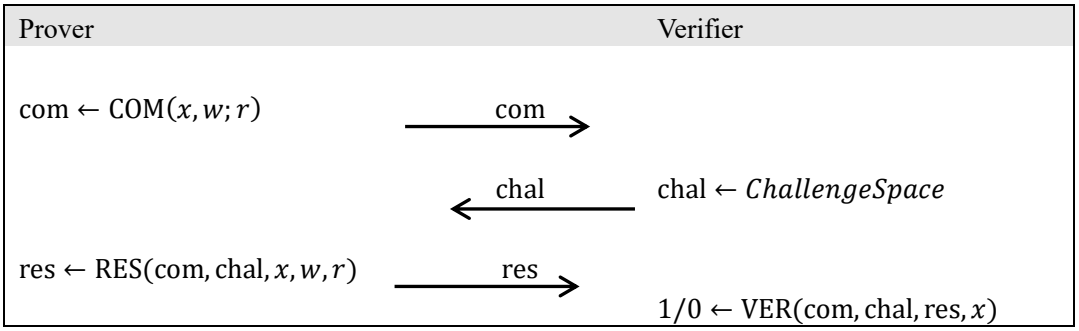


Figure A-4: Σ Protocol

Additionally, the function $\mathrm{EXT}(x, \mathrm{com}, \mathrm{chal}, \mathrm{chal}', \mathrm{res}, \mathrm{res}')$ returns the witness w satisfying $\mathrm{com} \leftarrow \mathrm{COM}(x, w; r)$ from the inputs $(\mathrm{chal}, \mathrm{res})$ and $(\mathrm{chal}', \mathrm{res}')$, which use the same commitment in two zero-knowledge proofs.

The above Σ protocol can be converted into a non-interactive proof using hash function H. Specifically, replacing $\mathrm{chal} \leftarrow H(\mathrm{com})$ allows the prover to generate res without interacting with the verifier.

The privacy-enhanced electronic signature scheme is composed of the following functions:

- $(\mathrm{sk}, \mathrm{pk}) \leftarrow \mathrm{Gen}(1^{\delta})$: Gen generates a key pair $(\mathrm{sk}, \mathrm{pk})$, where sk is the private key and pk is the public key. δ is the security parameter.
- $c \leftarrow \mathrm{Commit}(x; r)$: Commit generates a commitment c for x using a random number r.
- $\sigma \leftarrow \mathrm{Sign}_{\mathrm{sk}}(m)$: Sign generates a digital signature σ for the message m using the private key sk.
- $1/0 \leftarrow \mathrm{Verify}_{\mathrm{pk}}(m, \sigma)$: Verify verifies the digital signature σ of the message m using the public key pk. It outputs 1 if σ is a valid signature and 0 otherwise.
- $\mathrm{com} \leftarrow \mathrm{COM}(x, w; r)$: COM generates a commitment com for the witness w of x in the Σ protocol to prove the possession of the witness w for x. r is a random number.
- $\mathrm{chal} \leftarrow H(\mathrm{com})$: H is a hash function used to generate challenges in the Σ protocol.
- $\mathrm{res} \leftarrow \mathrm{RES}(\mathrm{com}, \mathrm{chal}, x, w, r)$: RES generates a response res in the Σ protocol to prove the possession of the witness w for x.
- $1/0 \leftarrow \mathrm{VER}(\mathrm{com}, \mathrm{chal}, \mathrm{res}, x)$: VER verifies whether com and res is a valid pair in the Σ protocol to prove the possession of the witness w for x. It outputs 1 if $(\mathrm{com}, \mathrm{res})$ are valid and 0 otherwise.
- $w \leftarrow \mathrm{EXT}(x, \mathrm{com}, \mathrm{chal}, \mathrm{chal}', \mathrm{res}, \mathrm{res}')$: EXT extracts the witness w satisfying $\mathrm{com} \leftarrow \mathrm{COM}(x, w; r)$ from the inputs $(\mathrm{chal}, \mathrm{res})$ and $(\mathrm{chal}', \mathrm{res}')$, which use the same commitment in two zero-knowledge proofs.

(2) Three implementation methods

Method 1 (Registering the private key with the certification authority and identifying double-spending users via the private key)

Method 1 involves registering the user's private key sk with the certification authority instead of the public key pk. The certification authority then issues a certificate Cer for the private key

sk. The three requirements outlined in Chapter 4 (4) are satisfied using the methods described below:

- Generation and update of transaction-specific public key $\mathrm{pk}_{(i)}$: Users generate their own transaction-specific public keys and update them for each i-th transaction. Transaction-specific public key $\mathrm{pk}_{(i)}$ is generated based on the private key sk.
- Certificate issuance for the private key: The user obtains a certificate Cer for the private key sk from the certification authority. By proving that both Cer and $\mathrm{pk}_{(i)}$ are derived from the same private key, it is demonstrated that transactions using $\mathrm{pk}_{(i)}$ are conducted by the legitimate user registered with the certification authority. Additionally, by utilizing zero-knowledge proof, both the private key sk and the certificate Cer can remain concealed, thereby satisfying anonymity requirements for service providers.
- Identification of fraudulent users by service providers: Service providers can leverage the characteristics of zero-knowledge proof to identify the private key sk of users who have engaged in double spending of electronic cash.

(i) Initial setup

The certification authority and users prepare the key pairs and the certificates as follows:

1. Certification authority C generates a pair of private and public keys, $(\mathrm{sk}_C, \mathrm{pk}_C) \leftarrow \mathrm{Gen}(1^\delta)$, and publishes the public key along with its self-signed certificate.
2. Certification authority C randomly selects the private key $\mathrm{sk}_U \in \{0,1\}^\lambda$ for user U, and issues $\mathrm{Cer}_U \leftarrow \mathrm{Sign}_{\mathrm{sk}_C}(\mathrm{sk}_U)$ to user U through a secure channel. Here, λ is the security parameter.
3. User U computes $\mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{sk}_U, \mathrm{Cer}_U)$. If the result is 1, the user accepts $(\mathrm{sk}_U, \mathrm{Cer}_U)$; otherwise, rejects it.

(ii) Receipt of electronic cash

A process user U receives electronic cash T from user V is as follows:

1. User U selects a random number $r_{U(i)} \in \{0,1\}^\lambda$ and computes transaction-specific public key $\mathrm{pk}_{U(i)} \leftarrow \mathrm{Commit}(\mathrm{sk}_U; r_{U(i)})$.
   - $\mathrm{pk}_{U(i)}$ is the public key used by user U for the i-th transaction.
2. User U selects another random number $r_{(i)} \in \{0,1\}^\lambda$ and computes $\mathrm{com}_{(i)} \leftarrow \mathrm{COM}((\mathrm{pk}_{U(i)}, \mathrm{pk}_C), (\mathrm{sk}_U, \mathrm{Cer}_U, r_{U(i)}); r_{(i)})$.
3. User U sends $(\mathrm{pk}_{U(i)}, \mathrm{com}_{(i)})$ to user V and receives $(T, \{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n \geq 0})$, along with the transaction-specific public keys of previous users in the transfer record, from user V. Here, T is the electronic cash issued by user V and signed with its serial

number by the service provider. $\sigma_{(n)}$ represents the transfer record of T, where n indicates the number of previous transfers of T.

- $\mathrm{com}_{(k)}$ is generated by user V upon receiving T from another user under the public key $\mathrm{pk}_{V(k)}$ (corresponding to Step 2 of this protocol performed by user U). It represents the k-th transaction for user V.
- $\mathrm{res}_{(k)}$ is generated by user V upon receiving $(\mathrm{pk}_{U(i)}, \mathrm{com}_{(i)})$ from user U (corresponding to Step 3 of protocol for sending electronic cash performed by user U).

4. User U verifies T and computes $\mathrm{VER}(\mathrm{com}_{(k)}, \mathrm{chal}_{(k)}, \mathrm{res}_{(k)}, (\mathrm{pk}_{V(k)}, \mathrm{pk}_C))$ for $\{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0}$. If all results are 1, the user accepts the electronic cash, otherwise, rejects it. Here, $\mathrm{chal}_{(k)} \leftarrow H(\mathrm{com}_{(k)})$ is the hash value of $\mathrm{com}_{(k)}$.

(iii) Transmission of electronic cash

A process user U sends electronic cash T to user W is as follows:

1. User U receives $(\mathrm{pk}_{W(j)}, \mathrm{com}_{(j)})$ from user W.
   - For user W, this corresponds to Steps 1–2 of the protocol for receiving electronic cash and represents the j-th transaction.
2. User U computes $\mathrm{chal}_{(i)} \leftarrow H(T, \mathrm{pk}_{W(j)}, \mathrm{com}_{(j)}, \mathrm{com}_{(i)})$.
   - $\mathrm{com}_{(i)}$ is generated by user U upon receiving T from user V (Step 2 of the protocol for receiving electronic cash).
3. User U computes $\mathrm{res}_{(i)} \leftarrow \mathrm{RES}(\mathrm{com}_{(i)}, \mathrm{chal}_{(i)}, (\mathrm{pk}_{U(i)}, \mathrm{pk}_C), (\mathrm{sk}_U, \mathrm{Cer}_U, r_{U(i)}), r_{(i)})$. The Σ protocol proves that $(\mathrm{pk}_{U(i)}, \mathrm{pk}_C)$ belong to the following language L:

$$\boldsymbol{L} \coloneqq \{(\mathbf{pk}_{U(i)}, \mathbf{pk}_C) | \exists (\mathbf{sk}_U, \mathbf{Cer}_U, \boldsymbol{r}_{U(i)}), \mathbf{com}(\mathbf{sk}_U; \boldsymbol{r}_{U(i)}) = \mathbf{pk}_{U(i)} \wedge \mathbf{Verify}_{\mathbf{pk}_C}(\mathbf{sk}_U, \mathbf{Cer}_U) = \mathbf{1}\}$$

4. User U sends $(T, \{\sigma_{(n+1)} = (\mathrm{com}_{(i)}, \mathrm{res}_{(i)})\}_{n\geq 0})$, along with the transaction-specific public keys of previous users in the transfer record, to user W.
5. User W verifies T and computes $\mathrm{VER}(\mathrm{com}_{(i)}, \mathrm{chal}_{(i)}, \mathrm{res}_{(i)}, (\mathrm{pk}_{U(i)}, \mathrm{pk}_C))$ for $\{\sigma_{(n+1)} = (\mathrm{com}_{(i)}, \mathrm{res}_{(i)})\}_{n\geq 0}$. If all results are 1, the user accepts the electronic cash; otherwise, rejects it. Here, $\mathrm{chal}_{(i)} \leftarrow H(\mathrm{com}_{(i)})$ is the hash value of $\mathrm{com}_{(i)}$.

(iv) Detection of double spending

A process the service provider identifies the double-spend of electronic cash is as follows:

1. If the serial number of the returned electronic cash T is not in the Issued Electronic Cash DB, the service provider determines that it has been double spent and retrieves T and its record σ' with the same serial number from the Redeemed Electronic Cash DB.

2. The service provider computes the private key $\mathrm{sk}_U \leftarrow \mathrm{Ext}(\mathrm{pk}_{U(i)}, \mathrm{com}, \mathrm{chal}, \mathrm{chal}', \mathrm{res}, \mathrm{res}')$ based on the two transfer records σ and σ'.
3. By inquiring with the certification authority, the service provider identifies the user associated with private key sk_U.

Method 2 (Registering the public key with the certification authority and identifying double-spending users via the private key)

Method 2 involves the issuance of a certificate for a user's public key rather than their private key. As no transmission of private keys occurs between the certification authority and the user, the risk of key leakage is reduced. However, the computational cost associated with the transmission and receipt of electronic cash increases compared to Method 1. The three requirements outlined in Chapter 4 (4) are satisfied using the methods described below:

- Generation and update of transaction-specific public keys: The user geerates the transaction-specific public key $\mathrm{pk}_{(i)}$ and updates it for each i-th transaction.
- Issuance of public key certificates: The user obtains a certificate Cer issued by the certification authority for their public key pk. By demonstrating that the transaction-specific public key $\mathrm{pk}_{(i)}$ and the public key pk are both derived from the same private key, it can be proven that the transaction using $\mathrm{pk}_{(i)}$ was conducted by a legitimate user registered with the certification authority.
  - The key difference from Method 1 is that the certificate issued by the certification authority applies to the public key. Consequently, the propositions to be proven under the Σ protocol differ, requiring changes to the generation methods for commitments and responses.
- Identification of fraudulent users by service providers: Service providers can leverage the characteristics of zero-knowledge proof to identify the private key sk of users who have engaged in double spending of electronic cash.

(i) Initial setup

The certification authority and users prepare the key pairs and the certificates as follows:

1. Certification authority C generates a pair of private and public keys, $(\mathrm{sk}_C, \mathrm{pk}_C) \leftarrow \mathrm{Gen}(1^\delta)$, and publishes the public key along with its self-signed certificate.
2. User U randomly selects private key $\mathrm{sk}_U \in \{0,1\}^\lambda$.
3. User U selects a random value r_U and computes the public key $pk_U \longleftarrow \mathrm{Commit}(\mathrm{sk}_U; r_U)$.

4. User U sends pk_U to the service provider and receives certificate $\mathrm{Cer}_U \leftarrow \mathrm{Sign}_{\mathrm{sk}_C}(\mathrm{pk}_U \| *)$ for pk_U.
5. User U verifies Cer_U by calculating $\mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_U, \mathrm{Cer}_U)$. If the result is 1, the user accepts $(\mathrm{pk}_U, \mathrm{Cer}_U)$; otherwise, rejects them.

(ii) Receipt of electronic cash

A process user U receives electronic cash T from user V is as follows:

1. User U selects a random value $r_{U(i)} \in \{0,1\}^\lambda$ and computes the transaction-specific public key $\mathrm{pk}_{\mathrm{U}(i)} \leftarrow \mathrm{Commit}(\mathrm{sk}_U; r_{U(i)})$.
2. User U selects another random value $r_{(i)} \in \{0,1\}^\lambda$ and computes $\mathrm{com}_{(i)} \leftarrow \mathrm{COM}((\mathrm{pk}_{U(i)}, \mathrm{pk}_C), (\mathrm{pk}_U, \mathrm{sk}_U, \mathrm{Cer}_U, r_{U(i)}, r_U); r_{(i)})$.
3. User U sends $(\mathrm{pk}_{U(i)}, \mathrm{com}_{(i)})$ to user V and receives $(T, \{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0})$, along with the transaction-specific public keys of previous users in the transfer record, from user V.
4. User U verifies T and calculates $\mathrm{VER}(\mathrm{com}_{(k)}, \mathrm{chal}_{(k)}, \mathrm{res}_{(k)}, (\mathrm{pk}_{V(k)}, \mathrm{pk}_C))$ for $\{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0}$. If all results are 1, the user accepts the electronic cash; otherwise, rejects it. Here, $\mathrm{chal}_{(k)} \leftarrow H(\mathrm{com}_{(k)})$ is the hash value of $\mathrm{com}_{(k)}$.

(iii) Transmission of electronic cash

A process user U sends electronic cash T to user W is as follows:

1. User U receives $(\mathrm{pk}_{W(j)}, \mathrm{com}_{(j)})$ from user W.
2. User U calculates $\mathrm{chal}_{(i)} \leftarrow H(T, \mathrm{pk}_{W(j)}, \mathrm{com}_{(j)}, \mathrm{com}_{(i)})$.
   - ✓ $\mathrm{com}_{(i)}$ is generated by user U upon receiving T from user V (Step 2 of the protocol for receiving electronic cash).
3. User U calculates $\mathrm{res}_{(i)} \leftarrow \mathrm{RES}(\mathrm{com}_{(i)}, \mathrm{chal}_{(i)}, (\mathrm{pk}_{U(i)}, \mathrm{pk}_C), (\mathrm{pk}_U, \mathrm{sk}_U, \mathrm{Cer}_U, r_{U(i)}, r_U), r_{(i)})$. The Σ protocol proves that $(\mathrm{pk}_{U(i)}, \mathrm{pk}_C)$ belong to the following language L: $L := \{(\mathrm{pk}_{U(i)}, \mathrm{pk}_C) | \exists (\mathrm{pk}_U, \mathrm{sk}_U, \mathrm{Cer}_U, r_{U(i)}, r_U), \mathrm{Commit}(\mathrm{sk}_U; r_{U(i)}) = \mathrm{pk}_{U(i)} \wedge \mathrm{Commit}(\mathrm{sk}_U; r_U) = \mathrm{pk}_U \wedge \mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_U, \mathrm{Cer}_U) = 1\}$.
4. User U sends $(T, \{\sigma_{(n+1)} = (\mathrm{com}_{(i)}, \mathrm{res}_{(i)})\}_{n\geq 0})$, along with the transaction-specific public keys of previous users in the transfer record, to user W.
5. User W verifies T and calculates $\mathrm{VER}(\mathrm{com}_{(i)}, \mathrm{chal}_{(i)}, \mathrm{res}_{(i)}, (\mathrm{pk}_{U(i)}, \mathrm{pk}_C))$ for all $\{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0}$. If all results are 1, the user accepts the electronic cash; otherwise, rejects it. Here, $\mathrm{chal}_{(i)} \leftarrow H(\mathrm{com}_{(i)})$ is the hash value of $\mathrm{com}_{(i)}$.

(iv) Detection of double spending

A process the service provider identifies the double-spend of electronic cash is as follows:

1. If the serial number of the returned electronic cash T is not in the Issued Electronic Cash DB, the service provider determines that it has been double spent and retrieves T and its circulation record σ' with the same serial number from the Redeemed Electronic Cash DB.
2. The service provider computes $\mathrm{sk}_U \leftarrow \mathrm{Ext}(\mathrm{pk}_{U(i)}, \mathrm{com}, \mathrm{chal}, \mathrm{chal}', \mathrm{res}, \mathrm{res}')$ based on the two transfer records σ and σ'.
3. By inquiring with the certification authority, the service provider identifies the user associated with private key sk_U.

The method introduced in Chapter 4 (Registering the public key with the certification authority and identifying double-spending users via the public key)

Detection of double spending in Methods 1 and 2 relies on exposing the private key that was fraudulently used to identify the user. However, since anyone who has the two electronic cash involved in double spending can expose the private key, there is a risk that the user who obtained the private key may conduct further fraudulent acts. In contrast, this method is characterized by the ability to identify the offending user solely through public information.

(i) Initial setup

The certification authority and users prepare the key pairs and the certificates as follows:

1. Certification authority C generates a pair of private and public keys, $(\mathrm{sk}_C, \mathrm{pk}_C) \leftarrow \mathrm{Gen}(1^\delta)$, and publishes them together with its self-signed certificate.
2. User U generates a pair of private and public keys, $(\mathrm{sk}_U, \mathrm{pk}_U) \leftarrow \mathrm{Gen}(1^\delta)$.
3. User U sends their public key pk_U to certification authority C, and receives certificate $\mathrm{Cer}_U \leftarrow \mathrm{Sign}_{\mathrm{sk}_C}(\mathrm{pk}_U \| *)$ for pk_U.
4. User U computes $\mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_U, \mathrm{Cer}_U)$, and accepts $(\mathrm{pk}_U, \mathrm{Cer}_U)$ if the result is 1, otherwise, rejects it.

(ii) Receipt of electronic cash

A process user U receives electronic cash T from user V is as follows:

1. User U randomly selects a transaction-specific public key $\mathrm{pk}_{U(i)} \in \{0,1\}^\lambda$.
2. User U computes $\mathrm{Cer}_{U(i)} \leftarrow \mathrm{Sign}_{\mathrm{sk}_U}(\mathrm{pk}_{U(i)})$.

3. User U selects a random value $r_{(i)} \in \{0,1\}^{\lambda}$ and computes $\mathrm{com}_{(i)} \leftarrow \mathrm{COM}((\mathrm{pk}_{U(i)}, \mathrm{pk}_C), (\mathrm{pk}_U, \mathrm{Cer}_{U(i)}, \mathrm{Cer}_U); r_{(i)})$.
4. User U sends $(\mathrm{pk}_{U(i)}, \mathrm{com}_{(i)})$ to user V and receives $(T, \{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0})$, along with the transaction-specific public keys of previous users in the transfer record, from user V.
5. User U verifies T and computes $\mathrm{VER}(\mathrm{com}_{(k)}, \mathrm{chal}_{(k)}, \mathrm{res}_{(k)}, (\mathrm{pk}_{V(k)}, \mathrm{pk}_C))$ for $\{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0}$. If all results are 1, the user accepts the electronic cash, otherwise, rejects it.

(iii) Transmission of electronic cash

A process user U sends electronic cash T to user W is as follows:

1. User U receives $(\mathrm{pk}_{W(j)}, \mathrm{com}_{(j)})$ from user W.
2. User U computes $\mathrm{chal}_{(i)} \leftarrow H(T, \mathrm{pk}_{W(j)}, \mathrm{com}_{(j)}, \mathrm{com}_{(i)})$.
   - $\mathrm{com}_{(i)}$ is generated by user U upon receiving the electronic cash T from user V (refer to Step 3 of the protocol for receiving electronic cash).
3. User U computes $\mathrm{res}_{(i)} \leftarrow \mathrm{RES}(\mathrm{com}_{(i)}, \mathrm{chal}_{(i)}, (\mathrm{pk}_{U(i)}, \mathrm{pk}_C), (\mathrm{pk}_U, \mathrm{Cer}_{U(i)}, \mathrm{Cer}_U))$. The Σ protocol proves that $(\mathrm{pk}_{U(i)}, \mathrm{pk}_C)$ belong to the following language L:

   $L \coloneqq \{(\mathrm{pk}_{U(i)}, \mathrm{pk}_C) | \exists (\mathrm{pk}_U, \mathrm{Cer}_{U(i)}, \mathrm{Cer}_U),\ \mathrm{Verify}_{\mathrm{pk}_U}(\mathrm{pk}_{U(i)}, \mathrm{Cer}_{U(i)}) = 1 \wedge \mathrm{Verify}_{\mathrm{pk}_C}(\mathrm{pk}_U, \mathrm{Cer}_U) = 1\}$.
4. User U sends $(T, \{\sigma_{(n+1)} = (\mathrm{com}_{(i)}, \mathrm{res}_{(i)})\}_{n\geq 0})$, along with the transaction-specific public keys of previous users in the transfer record, to user W.
5. User W verifies T and computes $\mathrm{VER}(\mathrm{com}_{(i)}, \mathrm{chal}_{(i)}, \mathrm{res}_{(i)}, (\mathrm{pk}_{U(i)}, \mathrm{pk}_C))$ for $\{\sigma_{(n)} = (\mathrm{com}_{(k)}, \mathrm{res}_{(k)})\}_{n\geq 0}$. If all results are 1, the user accepts the electronic cash, otherwise, rejects it.

(iv) Detection of double spending

A process the service provider identifies the double-spend of electronic cash is as follows:

1. If the serial number of the returned electronic cash T is not in the Issued Electronic Cash DB, the service provider determines that it has been double spent and retrieves T and its circulation record σ' with the same serial number from the Redeemed Electronic Cash DB.
2. The service provider computes $\mathrm{pk}_U \leftarrow \mathrm{Ext}(\mathrm{pk}_{U(i)}, \mathrm{com}, \mathrm{chal}, \mathrm{chal}', \mathrm{res}, \mathrm{res}')$ from the two transaction records σ and σ'.
3. By inquiring with the certification authority, the service provider identifies the user associated with public key pk_U.