Journal of Information Processing Vol.23 No.5 633–645 (Sep. 2015)

[DOI: 10.2197/ipsjjip.23.633]

Regular Paper

Study on the Feasibility of Smart-Banknotes

Hisao Sakazaki[1,a)] Yasuko Fukuzawa[1,b)]

Received: October 29, 2014, Accepted: June 5, 2015

Abstract: A large number of counterfeit banknotes have been found around the world. Every possible effort must therefore be made to prevent counterfeit banknotes. We focus on NFC technology as a new countermeasure against these threats. A banknote-authentication system using NFC-tags and smartphones called a "smart-banknote system"-was developed. The smart-banknote system has three anti-counterfeiting functions, and distinguishes legitimate banknotes from counterfeit ones. The effectiveness of the system was evaluated by fault tree analysis and flow model analysis. The evaluation shows the smart-banknote system is most effective against low-level counterfeiters and is reasonably effective against high-level counterfeiters. In this paper, we report a summary of the smart-banknote system and an evaluation of the effectiveness of the system.

Keywords: smart-banknote, counterfeit, RFID, NFC, smartphone

1. Introduction

A large number of counterfeit banknotes have been found around the world. **Table 1** lists the number of bills, total amount monetary value, and the ratio of total amount monetary value to nominal GDP [9], [10], [11], [12], [13], [14]. The ratio of the total amount monetary value to nominal GDP in recent years is plotted in **Fig. 1**. The figure shows that 80–300 times more counterfeit banknotes have been discovered in countries other than Japan.

To maintain healthy economies, it is important to maintain the value of the currency of a country as appropriate. Every possible effort must therefore be made to prevent counterfeit banknotes. Accordingly, the latest anti-counterfeiting technology, such as microprint, intaglio printing, latent images, watermark, magnetic ink and hologram images, have been implemented in new banknotes. Over the years, counterfeiting banknotes required considerable artistic and technical skills. Recently, because of the ubiquity of home computers and printers, casual computer users can produce high-quality counterfeit banknotes more easily. This type of counterfeiting requires neither artistic and technical skills nor a huge investment. These "easy-made" counterfeit banknotes have a huge impact on the integrity of currency.

The National Research Council investigated threats posed by counterfeiting banknotes [1]. It listed potential candidates (for example, chemical sensors [2], engineered cotton fiber [3], RFID [4]) for new countermeasures against these threats.

We focus on RFID technology among these candidates. Any effort to embed RFID-tags in banknotes must overcome such challenges as keeping RFID-tags thin. A new method of embedding RFID-tags has been developed in North Dakota State University [5], [6]. They use Laser-Enabled-Advanced-Packaging technology to assemble RFID-tags on paper. This technology can assemble semiconductor-chips with various thicknesses, including 350 μm/side, 20 μm thick [6]. Based upon the embedding RFID-tags technology, we assume that RFID-tags can be embedded in banknotes.

We might be able to embed RFID-tags in the banknotes using the above technology. However, it is not practical because banknotes can be handled very roughly, and the RFID-tags embedded in them might be easily damaged.

We describe the durability of the RFID-tag. With current technology, a 400 μm/side chip could be embedded in a paper by a paper machine [21], and in this case, the chip could withstand linear-pressure of 45 kgf/cm [21]. This pressure is much larger than the stress applied to the banknotes in daily life. Usami et al tested the mechanical strength of the RFID-tags [22]. According to the result, if the chip-size is 500 μm/side or less, the mechanical strength of the chip improves [22]. In the latest technology, Usami et al have succeeded in reducing the chip size to 50 μm/side [23], [24].

The Bank of Japan has not disclosed the durability requirement for banknotes. Moreover, the durability requirement may vary across countries. Although in this paper we cannot conclude whether the durability of the current chip is sufficient, the linear-pressure of 45 kgf/cm would be much larger than the stress applied to the banknotes in daily life. If the requirements of each country are higher than the linear-pressure of 45 kgf/cm, the chip will satisfy the requirements by reducing the chip-size in the future.

We show the data of water-resistance and heat-resistance of the current chip as well as the data of pressure-resistance. In regard to the data of water-resistance, some chips have passed a twenty-four-hour saltwater-dip-test and saltwater-spray-test [25]. In regard to the data of heat-resistance, the storage temperature of some chips is from −55°C to 126°C and the ambient temperature of them is from −25°C to 70°C [17], [18]. We assume that these

1 Hitachi, Ltd. Research & Development Group, Yokohama, Kanagawa 244–0817, Japan
a) hisao.sakazaki.qc@hitachi.com
b) yasuko.fukuzawa.pd@hitachi.com

Table 1 Number of counterfeit banknotes discovered.

	JAPAN [9]	**USA** [10]	**EURO** [11]	**ENGLAND** [12]	**BRASIL** [13]	**INDIA** [14]
1999	3,422 bills ¥28,740,000 $0.06*10^{-6}$	- $180,900,000 $19.45*10^{-6}$	- - -	- - -	- - -	37.523 bills Rs10,344,740 $0.52*10^{-6}$
2000	4,257 bills ¥32,489,000 $0.07*10^{-6}$	- $252,800,000 $25.54*10^{-6}$	- - -	- - -	- - -	102,687 bills Rs32,859,860 $1.59*10^{-6}$
2001	7,613 bills ¥41,576,000 $0.09*10^{-6}$	- $115,600,000 $11.30*10^{-6}$	- - -	- - -	- - -	124,515 bills Rs33,718,270 $1.47*10^{-6}$
2002	20,211 bills ¥84,567,000 $0.17*10^{-6}$	- $174,400,000 $16.39*10^{-6}$	- - -	439,000 bills £5,995,000 $5.61*10^{-6}$	- - -	211,754 bills Rs35,174,760 $1.56*10^{-6}$
2003	16,910 bills ¥76,639,000 $0.15*10^{-6}$	- $101,000,000 $9.06*10^{-6}$	- - -	381,000 bills £6,640,000 $5.84*10^{-6}$	- - -	205,226 bills Rs27,612,540 $1.09*10^{-6}$
2004	25,858 bills ¥109,349,000 $0.22*10^{-6}$	- $88,600,000 $7.47*10^{-6}$	594,000 bills €33,768,900 $3.18*10^{-6}$	332,000 bills £6,370,000 $5.31*10^{-6}$	- - -	181,928 bills Rs24,379,460 $0.82*10^{-6}$
2005	12,203 bills ¥65,864,000 $0.13*10^{-6}$	- $113,600,000 $9.00*10^{-6}$	579,000 bills €34,074,150 $3.08*10^{-6}$	502,000 bills £10,060,000 $7.97*10^{-6}$	- - -	123,917 bills Rs17,675,150 $0.52*10^{-6}$
2006	4,288 bills ¥34,931,000 $0.07*10^{-6}$	- - -	565,000 bills €27,261,205 $2.33*10^{-6}$	389,000 bills £7,760,000 $5.82*10^{-6}$	- - -	104,743 bills Rs23,190,300 $0.59*10^{-6}$
2007	15,779 bills ¥48,334,000 $0.09*10^{-6}$	- - -	561,000 bills €41,149,350 $3.32*10^{-6}$	298,000 bills £5,960,000 $4.22*10^{-6}$	671,169 bills R$25,740,888 $9.67*10^{-6}$	195,811 bills Rs54,991,180 $1.20*10^{-6}$
2008	2,540 bills ¥20,741,000 $0.04*10^{-6}$	- - -	666,000 bills €41,175,450 $3.30*10^{-6}$	687,000 bills £13,720,000 $9.52*10^{-6}$	534,332 bills R$22,440,541 $7.40*10^{-6}$	398,111 bills Rs155,705,000 $2.94*10^{-6}$
2009	3,433 bills ¥22,248,000 $0.05*10^{-6}$	- - -	860,000 bills €40,269,500 $3.43*10^{-6}$	570,000 bills £11,220,000 $8.00*10^{-6}$	501,925 bills R$25,037,438 $7.73*10^{-6}$	401,476 bills - -
2010	3,609 bills ¥27,675,000 $0.06*10^{-6}$	- - -	751,000 bills €35,465,975 $2.89*10^{-6}$	302,000 bills £5,930,000 $4.04*10^{-6}$	421,044 bills R$20,789,106 $5.51*10^{-6}$	435,607 bills - -
2011	1,536 bills ¥12,292,000 $0.03*10^{-6}$	- - -	606,000 bills €30,466,650 $2.41*10^{-6}$	374,000 bills £6,265,000 $4.12*10^{-6}$	426,758 bills R$23,801,888 $5.75*10^{-6}$	521,155 bills - -

(Number of bills, total amount monetary value, ratio of total amount monetary value to nominal GDP)

data indicate sufficient durability in daily life use[*1].

Then, we focus on the security evaluation of RFID-tag-embedded banknotes.

In particular, the development of Near-Field Communication (NFC) technology is remarkable. NFC-tag is a kind of RFID-tag. NFC is a short-range (a few centimeters) wireless connectivity technology and is a world-wide standard for NFC devices developed by the NFC Forum [16]. An NFC-tag is typically a passive device that does not contain a battery; the power is supplied by a radio wave from an NFC-tag reader. NFC-tag reader has become one of the standard features of a smartphone in recent years. According to Seed Planning, Inc., in 2015, the number of smartphones users will globally be 3.1 billions [19] and about 60% of newly-shipped smartphones will be NFC-enabled [20]. Authentication of banknotes using smartphones has therefore become a possibility. To establish these technological countermeasures and to evaluate their practicality, in this study, a banknote-authentication system, called a "smart-banknote system," which uses NFC-tags and smartphones, was developed. The effectiveness of the smart-banknote system was evaluated by fault tree analysis and flow model analysis. The evaluation by fault

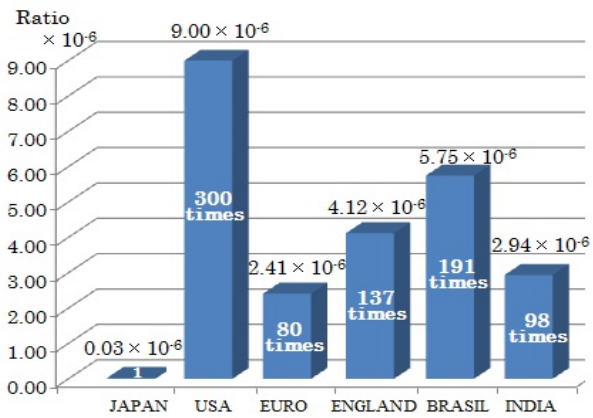

Fig. 1 Ratio of total amount monetary value to nominal GDP in recent years.

*1 The Bank of Japan has not disclosed the durability requirement for banknotes. Moreover, the durability requirement may vary across countries. Although in this paper we cannot conclude whether the durability of the current chip is sufficient, we assume that these data indicate sufficient durability in daily life use. In the future, we need to determine the durability-requirement for the RFID-tag embedded in a banknote in cooperation with authorities of each country.

Table 2 Relation between conventional anti-counterfeiting technologies and verification methods.

Verification methods	Example	Conventional anti-counterfeiting technologies
By human senses	senses of sight, touch	intaglio printing, latent images, watermark, hologram images
With portable auxiliary tools	loupe	microprint
By special machines	banknote counter	magnetic ink

Table 3 Comparison between NFC-tag, bar-code and digital-watermark.

	Advantage	Disadvantage
RFID-tag	Resistant to stains and scratch marks. Readable in darkness or beyond obstacles. No need to change the graphic design of banknotes.	More expensive than bar-code and digital-watermark. Possibility that NFC-tags are broken.
Bar-code	Less expensive than NFC.	Need to change the graphic design of the banknotes for bar-code. Vulnerable to stains and scratch marks.
Digital watermark	Less expensive than NFC. No need to change the graphic design of banknotes.	Vulnerable to stains and scratch marks.

tree analysis shows the smart-banknote system is most effective against low-level counterfeiters and is reasonably effective against high-level counterfeiters. The evaluation by flow model analysis estimates the steady-state amount of unused counterfeit smart-banknotes in stockpile and the steady-state amount of counterfeit smart-banknotes in circulation. These two evaluations are the main results in this paper.

This paper is organized as follows. Section 2 shows the definition of backgrounds and terms. Section 3 summarizes the smart-banknote system. Section 4 classifies the counterfeiter and evaluates countermeasures. Finally, Section 5 presents our conclusions.

2. Preparation

We define backgrounds and terms in this paper.

2.1 Life cycle of banknotes

(i) Production: banknotes are produced by a central bank[*2].
(ii) Issue: banknotes are issued by the central bank.
(iii) Circulation: banknotes are in circulation.
(iv) Withdrawal: banks withdraw banknotes from circulation. (for deposits, banknotes are collected to banks via ATM or bank counters.)
(v) Recirculation: banknotes are in circulation again.
(vi) Culling: after a certain period of time, old-banknotes are culled by a central bank.

Counterfeit banknotes are mainly used in phases "(iii) Circulation" and "(v) Recirculation."

2.2 Entities

- Central Bank: produces, issues and culls banknotes (in above phases (i), (ii) and (vi)).
- Banks: withdraw banknotes from circulation (in phase (iv)).
- User, Verifier: uses banknotes, and verifies validity of banknotes (in phases (iii), (v)). e.g., citizen, bank-clerk, ATM, vending-machines, shop and so forth.
- Police: investigate and seize counterfeit banknotes in circulation (in phases (iii), (v)).

2.3 Ability of Verifiers

2.3.1 Verifier Type

- Ordinary verifier: verifier without training (e.g., ordinary person, store clerk).
- Special verifier: verifier with specialty training (e.g., bank clerk, professional researcher).

2.3.2 Verification Method

- By human senses (e.g., senses of sight, touch).
- With portable auxiliary tools (e.g., loupe).
- By special machines (e.g., banknote counter).

Table 2 shows a relation between conventional anti-counterfeiting technologies and verification methods.

Our proposal targets ordinary verifiers with portable auxiliary tools[*3].

2.4 Comparison between RFID-tag, Bar-code and Digital-watermark

We focus on RFID technology as a new countermeasure against counterfeiting banknotes. RFID is a data-transfer technology for distant reading of codes. As the similar technologies of distant reading of codes, there are bar code and digital watermark. We compare these technologies. **Table 3** shows comparison between RFID-tag, bar-code and digital-watermark. RFID-tag is more expensive than bar-code and digital-watermark; however, it has an important advantage in read-stability of information from banknotes, for example, it is resistant to stains and scratch marks, as well as it is readable in darkness or beyond obstacles. Considering this advantage, RFID has been adopted as a candidate for anti-counterfeiting technology in our proposal.

2.5 Operational Design for Malfunctioning RFID-tags

Even if we use a durable RFID-tag (see Section 1), there is a possibility that the RFID-tag will malfunction. We need to define the operational design for the malfunctioning RFID-tag.

*2 In some countries, banknotes are produced not only by their central bank but also by their governmental organizations or private companies [28]. For simplicity, in this paper, the central bank is only regarded as the producer of banknotes. Please take the central bank as the governmental organizations or private companies as necessary.

*3 Although we use a smartphone as a tool, the proposed mechanism is applicable to a vending machine, ATM and POS terminal.

Currently, paper-based banknotes implement anti-counterfeiting technologies, such as microprint, intaglio printing, latent images, watermark, magnetic ink and hologram images. Even if one of these anti-counterfeiting technologies malfunctions, a banknote does not necessarily become a counterfeit one. For example, if we press a banknote with a hot-iron, the chemical property of hologram image is changed. In this case, the Bank of Japan has expressed their opinion that the value of the banknote as money still remains [30]. According to the Bank of Japan Act 48, the Bank of Japan exchanges mutilated banknotes for free [29]. In our proposal we assume it is a better operation that the authority exchanges the RFID-tag-malfunctioning banknote as is the case for mutilated banknote with damaged hologram-image. In this case, authentication by other anti-counterfeiting technologies, such as microprint, intaglio printing, latent images, watermark, magnetic ink and hologram images, is surely necessary.

There is also a method which reduces the probability that the RFID-tag embedded in a banknote malfunctions. For example, by embedding multiple chips in a single banknote, unless all chips malfunction the value of RFID-tag-embedded banknote as money still remain. Although the situation varies across countries, the average lifespan of banknotes in Japan is one to two years for 5,000 yen and 1,000 yen notes which are used more frequently, and four to five years for 10,000 yen notes [28]. By exchanging the banknotes in a few years before all chips malfunction, it is possible to reduce the probability that the malfunctioning RFID-tag-embedded banknotes go into circulation. If all the chips are broken in circulation, we think that the exchange of the mutilated banknote by the authority in a similar fashion is a better operation.

In this subsection, we have introduced the outline of the operational design for malfunctioning RFID-tags. However, the optimal operation varies across countries. We would like to investigate the condition of each country and to study the operational design for the RFID-tag-embedded-banknote more deeply in the future work.

2.6 Proposed Smart-banknote System

We define the following terms used in a smart-banknote system.

- smart-banknote: a banknote with a NFC-tag attached. In addition, a printed-serial-number is on the surface of the banknote.
- NFC-tag: an NFC-tag has a tag-serial-number, a system-version-number, a printed-serial-number, value of the banknote and digital signature data (see Fig. 3).
- Smartphone: a smartphone equips an NFC reader. Smartphones can verify the validity of smart-banknotes and communicate with a data center in a central bank via the internet/the mobile network.
- Vending machine, ATM, POS terminal: as a smartphone does, these devices verify validity of banknotes. These devices equip an NFC-reader and can communicate with the data center via the internet.
- Data center: the data center manages two databases (DB_1, DB_2).
- DB_1: DB_1 manages white-lists and black-lists.
- DB_2: DB_2 manages tag-serial-numbers, printed-serial-numbers, and verification time and location, (see Section 3.3.3 for details).
- White-list: tag/printed-serial-numbers of all legitimate banknotes in circulation.
- Black-list: tag/printed-serial-numbers of counterfeit banknotes.
- Local verification: a stand-alone device checks validity of smart-banknotes, without a network.
- Network authentication: a data center checks validity of smart-banknotes.

3. Smart-banknote System

3.1 Concept of Smart-banknote System

Using NFC-tags and smartphones, the smart-banknote system is designed on the basis of the following targets.

(1) Adding a new technology to conventional technologies such as microprint, watermark, magnetic ink and hologram images.
(2) Providing an environment in which users can easily verify banknotes.
(3) Implementing standard technologies that have not been developed for currency-related applications, since they can be more quickly implemented to provide an added measure of deterrence.

As for the first target, it is more effective to verify banknotes by a variety of techniques than by a single technique. We focus on strengthening counterfeit resistance by adding a new technology such as information and communication technology (ICT). Banknotes can easily be associated with related information (time, location, and so forth), by ICT (see Section 3.3.3).

As for the second target, it is also important that anyone can easily verify banknotes; thus, it is necessary to consider accessible devices. In recent years, a NFC-tag reader has become one of the standard features of a smartphone. Using a smartphone as a verification device can provide an environment in which users can easily verify banknotes.

As for the third target, it is expected that many standardized technologies will be commercialized in the near future. Standard technologies can be more quickly implemented to provide an additional countermeasure. However, there is also a disadvantage that an attacker is likely to easily use the standard technology. Nevertheless, by adopting standard technologies for banknotes, there is an advantage that a banknote-producer can obtain knowledge of counterfeit resistance from the prior case since standard technologies such as NFC-tag are used in the admission-tickets etc. Therefore, NFC technology has been adopted as a candidate for anti-counterfeiting technologies in our proposal[*4].

3.2 Overview of Smart-banknote System

In this study, a smart-banknote system was developed.

We discuss the effectiveness of our anti-counterfeiting technol-

[*4] Although we adopted NFC technology as a candidate for anti-counterfeiting technologies, it is not limited to NFC technology.

Table 4 Functions of anti-counterfeiting.

Function name	Meaning
Distinguish function	distinguish between legitimate banknotes and counterfeit ones
Validity-checking function	check whether a banknote is currently in circulation
Analytical function	analyze the distribution of counterfeit banknotes

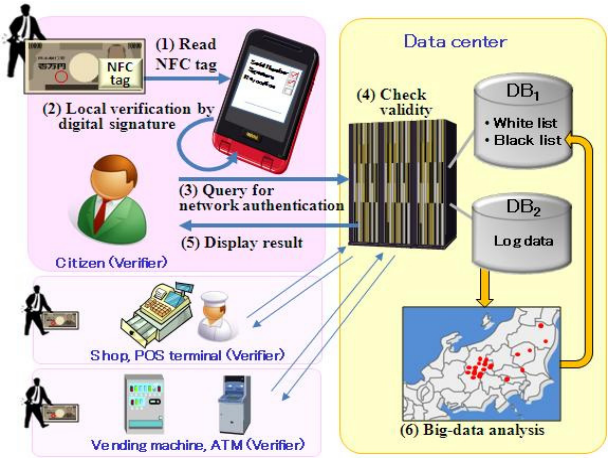

Fig. 2 Smart-banknote system.

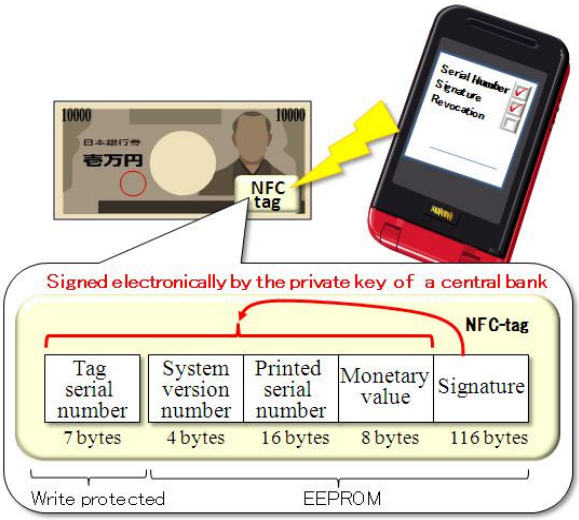

Fig. 3 Mechanism of digital-signature scheme used in the smart-banknote system.

ogy using the smart- banknote system. Since we evaluate our anti-counterfeiting technology, evaluation including conventional anti-counterfeiting technologies is outside the scope of our evaluation.

A smart-banknote is verified by the smart-banknote system with a smartphone. The system verifies smart-banknotes through the following processes (see **Fig. 2**).

(1) A verifier reads the information from a smart-banknote via a smartphone.
(2) A smart-banknote application starts up and verifies the digital signature of the smart-banknote (i.e., local verification).
(3) The application sends a query to a data center for network authentication[*5].
(4) The data center checks the validity of the tag/printed-serial-number of the smart-banknote.
(5) The verifier's smartphone displays the results from the data center.
(6) In parallel, the data center analyzes the distribution of counterfeit banknotes[*6].

3.3 Anti-counterfeiting Functions

The three main functions of anti-counterfeiting performed by the system are shown in **Table 4**.

3.3.1 Distinguish Function

The distinguish function distinguishes legitimate banknotes from counterfeit ones. It performs local verification that does not require a network. It is implemented by the conventional technologies such as microprint, intaglio printing, latent images, watermark, magnetic ink, and hologram images. In the proposed system, however, digital-signature technology is applied to implement this function. A verifier distinguishes legitimate banknotes from counterfeit ones by verifying the digital signature written in a NFC-tag (see Fig. 2 Step (1), (2)).

In our system, an RFID-tag [17] based on a NFC standard is applied. The tag operates at a frequency of 13.56 MHz and has a 192-byte memory in total. A unique 7-byte tag-serial-number is embedded in the first seven bytes of the memory. These bytes are write-protected after having been programmed by the IC manufacturer in the production process. The tag has a 144-byte user memory, to which write access can be permanently restricted by a read-only locking function. In regard to the proposed smart-banknote system, the central bank writes a system-version-number, the printed-serial-number, and a monetary value to the user memory of the tag. A digital signature is created by using a private key of the central bank, and the central bank writes a signature to the user memory. A signed message contains the tag-serial-number as well as the system-version-number, the printed-serial-number, and the monetary value (see **Fig. 3**). The system-version-number may be used to manage the date of production of banknotes; thus, it is not important in regard to security.

Since the user memory of this NFC-tag is small in practice, an elliptic-curve digital-signature algorithm (ECDSA) [26], whose digital-signature size is relatively small, is applied. The specific data structure of a smart-banknote is listed below.

- 7-byte tag-serial-number (write-protected),
- 4-byte system-version-number,
- 16-byte printed-serial-number,
- 8-byte value of the banknote,

*5 There are two ways in this step. One is a real-time processing to send a query to the data center at each time and another is a batch processing to send some queries to the data center at one time. The former can get the latest result, but cannot send a query to the data center from an area outside the radio wave range. The latter can send some queries to the data center at one time, when it is in the range, but may not get results on real-time.

*6 By performing step 6 before step 5, verifier can receive results of analysis on real-time.

- 116-byte signature data of ECDSA over secp224r1 [27].

If a counterfeiter produces banknotes with random data, steps in signature verification will fail. The distinguish function can distinguish counterfeit banknotes created with random data.

Based on the result of validation of ECDSA, the distinguish function distinguishes legitimate banknotes from counterfeit ones. If ECDSA is compromised and/or the private key of the central bank is leaked, this distinguish function will no longer work properly. In our proposal, we should change the signature scheme from ECDSA to new-ECDSA before ECDSA is compromised. For simplicity, "the optimal signature scheme at that time" is called "new-ECDSA" in this paper. The central bank is able to write a system-version-number to the user memory of the RFID-tag. The system-version-number of RFID-tag embedded in the newly issued banknote is updated. By referring to the system-serial-number, the distinguish function is able to find that the newly issued banknote is compatible with new-ECDSA.

Although the situation varies across countries, the average lifespan of banknotes in Japan is one to two years for 5,000 yen and 1,000 yen notes which are used more frequently, and four to five years for 10,000 yen notes [28]. By exchanging banknotes in a few years, it is possible to replace many ECDSA-based old-banknotes by new-ECDSA-based new-banknotes before ECDSA is compromised[*7]. There is a possibility that ECDSA-based hoarded-banknotes are used in the market after ECDSA is compromised. In this case, we think it is a better operation that ECDSA-based old banknotes are exchanged by the authority in a similar fashion.

On the other hand, if the private key of the central bank is leaked, the central bank immediately needs to replace these banknotes in the market. However, it is hard to replace all of these banknotes in the market at one time. So, we think that the private key should be updated within a certain period of time. In this case, even if the private key valid in a specific period is leaked, it is possible to reduce the impact on the market by replacing only the corresponding banknotes. In our system, the correspondence between the banknote and the secret key for a specific period can be associated with the system-version-number of the RFID-tag.

3.3.2 Validity-checking Function

The validity-checking function reduces the circulation of counterfeit banknotes by the checking tag/printed-serial-number of the smart-banknote (see Fig. 2 Step (3), (4), (5)). Its mechanism is as follows.

Firstly, the application on a verifier's smartphone sends a query to the data center for network authentication. The query is composed of the tag-serial-number, the printed-serial-number, time information and location information obtained by the global positioning system (GPS). Secondly, the data center checks a "white-list" containing the tag/printed-serial-numbers of all legitimate banknotes in circulation. Finally, the data center checks a "black-list" containing the tag/printed-serial-numbers of counterfeit banknotes.

The total amount of data size in each list was calculated. In the United States in 2011, the total monetary amount of currency in circulation was $1,043.5 billion (about 31.3 billion bills) [15]. Since the amount of data of a single record on the list is 23 bytes (i.e., 7-byte tag-serial-number/16-byte printed-serial-number), the total amount of data on the white-list is 719.9 G bytes (31.3 billion bills × 23 bytes). In the United States in 2000 [10], the total monetary amount of counterfeit banknotes was $252.8 million (about 5,056,000 bills[*8]); therefore, the total amount of data on the black-list is 116 M bytes/year (5,056,000 bills × 23 bytes). The data size of the black-list will be less than 1 G byte in 8 years, assuming that the volume of the black-list will increase at the same rate every year.

The white-list contains a relatively large amount of data; therefore, it is better that the data center manages the white-list. Since the black-list contains a relatively small amount of data, however, it can be sent to all verifiers' smartphones. As a result, the black-list can be checked and the digital signature can be verified at the same time[*9].

3.3.3 Analytical Function

The analytical function analyzes the distribution of counterfeit smart-banknotes (see Fig. 2 Step (6)). It also analyzes the history of usage of counterfeit smart-banknotes and detects unknown counterfeits.

The application on the verifier's smartphone sends a query to the data center for network authentication. The query is composed of the tag-serial-number, the printed-serial-number, time information and location information obtained by GPS. By associating the information of time and location with the tag/printed-serial-number of counterfeit banknotes, the analytical function can track the use of counterfeit smart-banknotes, and identify the areas where they are used. This function provides clues to criminal investigation of counterfeit smart-banknotes.

Moreover, if banknotes with the same tag/printed-serial-number are used at different locations at the same time, it is presumed that they are counterfeit banknotes; in other words, it is possible to detect unknown counterfeit banknotes.

4. Classification of Counterfeiters and Evaluation of Tolerability to Counterfeiting

4.1 Classification of Counterfeiters

The National Research Council [1] classified banknote counterfeiters into five levels. In this present study, however, it is modified in accordance with available RFID technologies. The modified definitions of classes of counterfeiters are listed in **Ta-**

*7 Retention time of NXP's MIFARE Ultralight C is 5 years [17], which is the same as the average lifespan of 10,000 yen. Retention time of NXP's new chip, NTAG213/215/216, is 10 years [18], which is twice as long as the average lifespan of 10,000 yen. In this paper, we have developed a prototype system using MIFAREUltralight C. According to the lifespan of the intended banknote, it may be better to use a chip which has a longer retention time.

*8 For the sake of simplicity, it is assumed that $50 banknotes have been forged, so the number of bills is calculated as $252.8 million/$50 = 5,056,000

*9 We assume that smartphones are able to store black-lists of 8 years. Since the system-version-number in the NFC-tag manages the date of production of smart-banknotes, a smartphone can read the date of production from the smart-banknote. In the case of the old smart-banknote (e.g., issued more than 8 years ago), the smartphone cannot check the validity of the smart-banknote using the black-list in the smartphone. Therefore, the smartphone should communicate with the data center, and check the validity of them using the black-list in the data center.

Table 5 Classes of banknote counterfeiters.

Level	Class	Typical practitioner	Primary tools
1	Primitive	Unusually motivated individual	Manual artistry/handicraft
2	Opportunist	Typically works alone	Home/office equipment, smartphone, RFID-Reader, and handicraft
3	Petty criminal	Criminal intent, typically works alone	Home/office equipment, smartphone, RFID-R/W plus NFC-tags on the market, and handicraft
4	Professional criminal	Criminal, trained in printing technology, often members of a criminal group	Offset printing, high-end ink-jet printers, smartphone, RFID-R/W plus specialty NFC-tags without tag-serial-number, and special adhesion technologies
5	State-sponsored	Professional, profiteer or terrorist, member of a large organization	All materials and processes, including specialty paper intaglio and offset printing, security features, smartphone, RFID-R/W plus specialty NFC-tags and cryptanalytic tools, and special adhesion technologies

ble 5 as five levels of smart-banknote counterfeiters.

Primitive counterfeiters may use manual artistry to modify a piece of currency in order to increase its money value and obtain financial gain. They forge banknotes by hand individually; therefore, their counterfeits are often apparently different from legitimate ones.

Opportunist counterfeiters work individually, making only a few banknotes at a time and printing them on home/office equipment. They can also use a PC, a smartphone, and a RFID reader; however, while they can handle NFC-tags, they can only strip the tags from legitimate banknotes and put them on counterfeit banknotes.

Petty-criminal counterfeiters have a clear and systematic intent to counterfeit repeatedly. They can also use a RFID writer and may use high-quality paper and inks. While handling with NFC-tags, they can buy NFC-tags on the market and write data to those tags with a RFID writer.

Professional-criminal counterfeiters produce counterfeit banknotes that are typically relatively easy to get into circulation. These counterfeiters are typically members of a larger criminal group that can include specialists who had professional training in the printing business. They establish an accessible route to special NFC-tags that have no tag-serial-number. They can write data, which include a tag-serial-number, to the tags freely and put those tags onto counterfeit banknotes without incongruity by using special adhesion technologies.

State-sponsored counterfeiters not only plan for criminal financial gain but may also have a political goal such as reducing global confidence in financial markets. Some state-sponsored organizations produce their own paper with watermarks and hologram images. They use the same printing methods, such as intaglio and letterpress, as legitimate organizations. They can also produce special NFC-tags that have no tag-serial-number and put those tags on counterfeit banknotes without incongruity by using special adhesion technologies. Furthermore, it is assumed that they can forge a digital signature by using cryptanalytic tools.

4.2 Evaluation of Tolerability to Counterfeiting

The counterfeiting of smart-banknotes was analyzed by fault-tree analysis (FTA). The results of the FTA are shown in **Fig. 4**. The steps involved in counterfeiting smart-banknotes are described below.

- Printing of banknotes (Fig. 4_2)
- Counterfeiting of NFC-tags (Fig. 4_3)
- Putting counterfeit tag on the banknote (Fig. 4_4)

Since the proposed smart-banknote system is based on the concept of adding ICTs to conventional technologies, the last two steps were evaluated in this study.

To counterfeit NFC-tags in smart-banknotes, NFC-tags were prepared and data was written into them. There are three ways of acquiring NFC-tags: stripping NFC-tags from legitimate smart-banknotes (Fig. 4_3.1.1), buying NFC-tags on the market (Fig. 4_3.1.2), buying or manufacturing special NFC-tags that have no tag-serial-number (Fig. 4_3.1.3).

There are two cases regarding writing data to NFC-tags: data indicating successful-signature-verification are generated (Fig. 4_3.2.1) or random data are generated (Fig. 4_3.2.2). Moreover, the former case has two possibilities as follows: Data is copied from legitimate smart-banknotes (Fig. 4_3.2.1.1) or a signature value indicating successful verification is calculated (Fig. 4_3.2.1.2).

There are two ways of putting the counterfeit tag on the banknote: advanced adhesion by special technologies (Fig. 4_4.1) or coarse adhesion by hand (Fig. 4_4.2).

4.2.1 Evaluation of Tolerability against Low-level Counterfeiters

The tolerability against low-level counterfeiters (namely, level-3 or lower) was evaluated. In the smart-banknote system, a digital signature is created by using a private key of the central bank. A signed message contains the tag-serial-number, the system-version-number, the printed-serial-number, and the monetary value. It is therefore possible to distinguish counterfeit banknotes with a random tag/printed-serial-number. However, if counterfeiters copy data from legitimate smart-banknotes and write them to special NFC-tags (Fig. 4_3.2.1.1), called "clone tags," it is not possible to distinguish legitimate smart-banknotes from counterfeit smart-banknotes. This is because steps in signature verification would succeed. However, commercially available NFC-tags are assigned a tag-serial-number in advance, so low-level counterfeiters cannot produce clone tags.

Low-level counterfeiters can strip NFC-tags from legitimate smart-banknotes (Fig. 4_3.1.1) and put them on counterfeit banknotes; however, they will not be able to use legitimate smart-banknotes since those tags are removed. It is therefore assumed

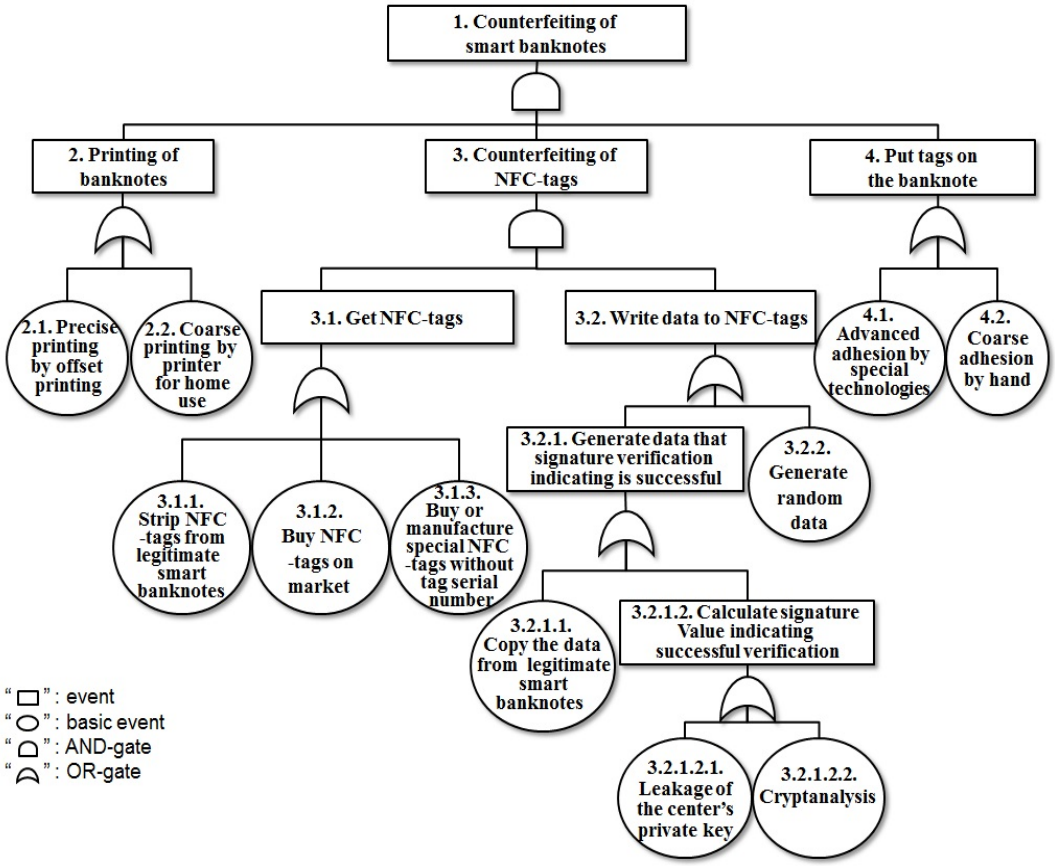

Fig. 4 Fault-tree analysis of counterfeit banknotes.

that the risk from this attack is negligible.

From the above consideration, under the assumption that it is not possible to rewrite the tag-serial-number in the NFC-tag, the smart-banknote system is very effective against low-level counterfeiters.

4.2.2 Evaluation of Tolerability against Level-4 Counterfeiters

Level-4 counterfeiters can buy or manufacture special NFC-tags without a tag-serial-number (Fig. 4_3.1.3), so they can produce clone tags. If they produce a lot of clone tags with different tag/printed-serial-numbers, they need a lot of data from legitimate smart-banknotes. Moreover, to print the printed-serial-numbers on banknotes, they need a lot of original plates. It is not efficient to produce a large amount of counterfeit smart-banknotes with different tag/printed-serial-numbers; therefore, level-4 counterfeiters might produce a large amount of cloned tags with the same tag/printed-serial-number.

In the case that many banknotes with the same tag/printed number are in circulation, if authorities such as a central bank or the police detect some of them as counterfeit smart-banknotes, they are able to update the tag/printed-serial-number to the black-list and inform every user through the network. It is possible to reduce economic loss by remaining counterfeit smart-banknotes with the same tag/printed-serial-number. With the smart-banknote system, the black-list can be easily checked by smartphones; this is the advantage of adding ICT to banknotes.

Moreover, if banknotes with the same tag/printed-serial-number are used at different locations at the same time, it is presumed that they are counterfeit banknotes. In other words, it is possible to detect unknown counterfeit banknotes.

Since level-4 counterfeiters can produce clone tags, the distinguish function of the smart-banknote system is ineffective; however, under the assumption that a large number of smart-banknotes with the same tag/printed-serial-number are in circulation, the validity-checking function and the analytical function are effective.

Level-4 counterfeiters can also strip NFC-tags from legitimate smart-banknotes (Fig. 4_3.1.1) and put them on counterfeit banknotes; however, since they can produce clone tags, this attack does not make sense. It is therefore assumed that the risk from this attack is negligible.

4.2.3 Evaluation of Tolerability against Level-5 Counterfeiters

It is assumed that level-5 counterfeiters can forge a digital signature by using cryptanalytic tools (Fig. 4_3.2.1.2.2). It is possible to produce counterfeit smart-banknotes with random tag/printed-serial-numbers whose digital-signature-verification-step will be successful; however, if these random tag/printed-serial-numbers are not present in the white-list, these counterfeit smart-banknotes can be detected by checking the white-list[*10]. These tag/printed-serial-numbers in the white-list cannot be easily counterfeited, as long as counterfeiters do not know the correct combination of tag-serial-number and printed-serial-number.

[*10] Even if these random tag/printed-serial-numbers are present in the white-list and also in the black-list, these counterfeit smart-banknotes can be detected by checking the black-list.

Table 6 Relation between methods of counterfeiting smart-banknotes and main counterfeiters.

Method of counterfeiting smart-banknote		Main counterfeiters
counterfeiting banknotes with no NFC-tags		Level-1
stripping NFC-tags from legitimate smart-banknotes and putting them on counterfeit banknotes		Level-2,3
counterfeiting smart-banknotes with invalid digital signature		Level-3
copying data from legitimate smart-banknotes and write them to special NFC-tags. counterfeiting smart-banknotes with "clone tags".	producing a large amount of counterfeit smart-banknotes with the same tag/printed-serial-number.	Level-4
	producing a large amount of counterfeit smart-banknotes with different tag/printed-serial-numbers	Level-5
forging a digital signature by using cryptanalytic tools, producing counterfeit smart-banknotes with random tag/printed-serial-numbers whose digital-signature-verification-step will be successful.		Level-5

Table 7 Evaluation of tolerability to counterfeiting.

Level & Class	Distinguish function	Validity-checking function	Analytical function
1: for primitive	very effective	—	—
2: for opportunist	very effective	—	—
3: for petty criminal	very effective	—	—
4: for professional criminal	ineffective	effective	effective
5: for state-sponsored	ineffective	ineffective	ineffective

"—": Only the distinguish function is fully effective.

If counterfeiters read data from a legitimate smart-banknote, they can know the correct combination of tag-serial-number and printed-serial-number, and consequently they can also get the correct value of digital signature at the same time, which means level-5's ability to forge digital signatures is not required for counterfeiting smart-banknote.

Level-5 counterfeiters can also produce clone tags using the same technique of level-4 counterfeiters. Since Level-5 counterfeiters can use the same printing methods, such as intaglio and letterpress, as legitimate organizations regardless of cost, they can produce a large amount of counterfeit smart-banknotes with different tag/printed-serial-numbers. If only a few smart-banknotes with same tag/printed-serial-numbers are in circulation, the probability that they are used in different locations at the same time decreases. The analytical function of the smart-banknote system is ineffective in this case. Therefore, it is difficult to reflect them to the black-list.

Table 6 shows the relation between method of counterfeiting smart-banknotes and main counterfeiters, and the evaluation of tolerability against all levels of counterfeiters is summarized in **Table 7**.

4.3 Effectiveness of Proposed Smart-banknote System

4.3.1 Flow Model for Counterfeiting

The National Research Council evaluated the amount of counterfeit banknotes by using a flow model [1]. In this paper, the flow model was modified for the smart-banknote system, and the amount of counterfeit smart-banknotes was evaluated. The modified flow model for counterfeit smart-banknotes is shown in **Fig. 5**. The counterfeiting threat can be represented as a basic flow system. A rectangle represents a state and an action, an arrow represents a transition, and a rounded rectangle represents a factor that counterfeit production is suppressed. The left side in Fig. 5 shows the life cycle of banknotes (see Section 2.1). The variables used in the flow model are defined in **Table 8**.

The basic flow system is described as follows. Counterfeiters attempt to produce counterfeit smart-banknotes (Fig. 5_1). Manufacturing volume is reduced according to the difficulty associated with anti-counterfeiting technologies and severity of laws. Counterfeit smart-banknotes are in stockpile, waiting for the first pass attempt (Fig. 5_2). Some of the stockpiled counterfeit smart-banknotes are seized by the police (Fig. 5_3). The remaining stockpile is used in circulation. Payments by counterfeit smart-banknotes are called "passing events" (Fig. 5_4), which are categorized into two cases. One is successful use, and the other is detection of counterfeits. In the former case, counterfeit smart-banknotes will be stay in circulation (Fig. 5_5). In the latter case, counterfeit smart-banknotes may be reported to a central bank (Fig. 5_6.1) or not reported (Fig. 5_6.2). Not-reported counterfeit smart-banknotes will be recirculated. After a certain period of time, all smart-banknotes, including legitimate ones and counterfeit ones, are culled by the central bank (Fig. 5_7).

To analyze the flow model, parameters should be defined. "p" means counterfeit production rate per unit time. The counterfeit production rate decreases according to "a," which means the difficulty associated with anti-counterfeiting technologies and the severity of laws and penalties. "x" means the number of unused counterfeit smart-banknotes that have been stockpiled. "x" is an important parameter for analyzing the flow model. "c" means the confiscation rate of unused counterfeit smart-banknotes from the stockpile. "c" is likely influenced most by law-enforcement activities. "ϕ" means the rate of the first attempts to use counterfeit smart-banknotes from the stockpile, and the number of counterfeit smart-banknotes that have been used in a unit time is "ϕ·x." "s" means the fraction of successful pass attempts; in other words, the fraction of detected pass attempts is "(1 − s)." "r" means the fraction of detected and reported pass attempts. "h" means the fraction of pass attempts that are detected but not

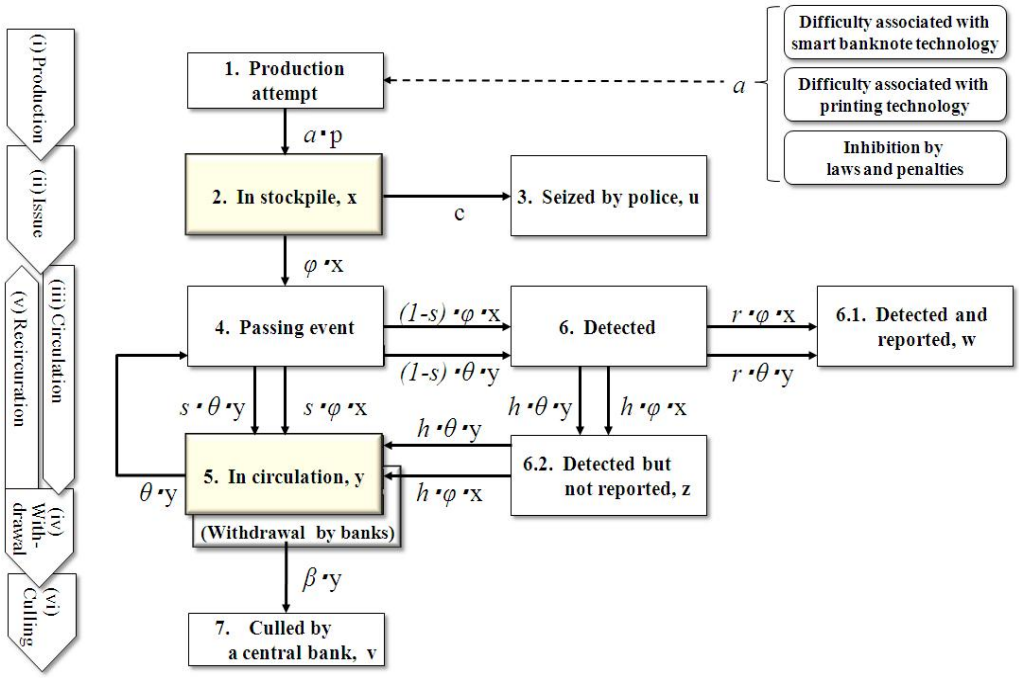

Fig. 5 Flow model for counterfeiting.

Table 8 Variables in the flow model for counterfeiting.

Variables	Definition
u=u(t)	Number of unused counterfeit banknotes that are seized by police
v=v(t)	Number of counterfeit banknotes that were culled by central bank
w=w(t)	Number of counterfeit banknotes that are detected and reported
x=x(t)	Number of unused counterfeit banknotes that are stockpiled
y=y(t)	Number of counterfeit banknotes that are circulating
z=z(t)	Number of counterfeit banknotes that are detected but not reported
c	Confiscation rate of unused counterfeit banknotes from stockpile (per unit time)
p	Counterfeit production rate (per unit time)
β	Rate of culling by central bank (per unit time)
ϕ	Rate of first attempts to use counterfeit smart-banknotes from stockpile (per unit time)
θ	Rate of attempts to repass counterfeit banknotes into circulation (per unit time)
a	Coefficient representing a decrease of production ($0 \le a \le 1$)
h	Fraction of pass attempts that are detected but not reported ($0 \le h \le 1$)
r	Fraction of pass attempts that are detected and reported ($0 \le r \le 1$)
s	Fraction of successful pass attempts ($1 = h + r + s$)
t	Time since start of production

reported. If counterfeit smart-banknotes are reported to the central bank, the central bank updates the black-list. As a result, "s" is reduced. Therefore, if counterfeit smart-banknotes with the same tag/printed-serial-number are in circulation (in "4. Passing event"), as the probability of "6. Detected" increases, the probability of "5. In circulation" decreases. "y" means the number of counterfeit smart-banknotes in circulation. Note that "y" is the most important parameter for analyzing the flow model. θ means the rate of attempts to repass counterfeit banknotes into circulation, and the number of counterfeit smart-banknotes that have been reused in unit time is "$\phi \cdot$ y." "β" means the rate of culling by the central bank after a certain period of time, where $\beta \cdot$ y bills of counterfeit smart-banknotes are culled by the central bank.

4.3.2 Effectiveness of the System over the Flow Model

With the aid of the flow model, reduction of counterfeit smart-banknotes in the smart-banknote system was evaluated.

The steady-state amount of unused counterfeit smart-banknotes in stockpile, "x(∞)," and the steady-state amount of counterfeits in circulation, "y(∞)," are given by the following equations.

Theorem

$$\mathrm{x}(t=\infty) = \frac{a \cdot \mathrm{p} - \mathrm{c}}{\phi} \tag{1}$$

$$\mathrm{y}(t=\infty) = \frac{(s+h) \cdot (a \cdot \mathrm{p} - \mathrm{c})}{r \cdot \theta + \beta} \tag{2}$$

proof

$$\frac{d\mathrm{x}}{dt} = a \cdot \mathrm{p} - \mathrm{c} - \phi \cdot \mathrm{x}(t),$$

$$\mathrm{x}(t) = \frac{a \cdot \mathrm{p} - \mathrm{c}}{\phi}[1 - e^{-\phi \cdot t}],$$

$$\mathrm{x}(\infty) = \frac{a \cdot \mathrm{p} - \mathrm{c}}{\phi}.$$

$$\frac{d\mathrm{y}}{dt} = s \cdot \phi \cdot \mathrm{x}(t) + s \cdot \theta \cdot \mathrm{y}(t) + h \cdot \theta \cdot \mathrm{y}(t) + h \cdot \phi \cdot \mathrm{x}(t) - \theta \cdot \mathrm{y}(t) - \beta \cdot \mathrm{y}(t),$$

$$= (s+h)\cdot\phi\cdot \mathrm{x}(t) - (r\cdot\theta+\beta)\cdot \mathrm{y}(t),$$

$$\mathrm{y}(t) = \frac{(s+h)\cdot(a\cdot \mathrm{p}-\mathrm{c})}{\phi-(r\cdot\theta+\beta)}\left[e^{-\phi\cdot t} - e^{-(r\cdot\theta+\beta)t} + \frac{\phi-(r\cdot\theta+\beta)}{(r\cdot\theta+\beta)}\right],$$

$$\mathrm{y}(\infty) = \frac{(s+h)\cdot(a\cdot \mathrm{p}-\mathrm{c})}{r\cdot\theta+\beta}.$$

q.e.d.

According to Eq. (1), the steady-state amount of unused counterfeit smart-banknotes in stockpile, "x(∞)" depends on the counterfeit production rate "$a\cdot$p," the confiscation rate "c," and the rate of the first attempt to use counterfeit smart-banknotes from stockpile, "ϕ." Since the confiscation rate is likely to be influenced most by law-enforcement activities, from the viewpoint of technological impact, the effects of "c" can be ignored. The ability of a feature to decrease the amount of unused counterfeit smart-banknotes in stockpile is related to its ability to do the following: (I) decrease the counterfeit production rate "$a\cdot$p" via the difficulty associated with anti-counterfeiting technologies, and (II) increase the rate of the first attempts to use counterfeit smart-banknotes from stockpile, "ϕ." However, doing (II) means increasing the number of counterfeit smart-banknotes in circulation; therefore, it is important to decrease the counterfeit production rate "$a\cdot$p."

On the other hand, according to Eq. (2), the ability of a feature to decrease the amount of counterfeits in circulation is related to its ability to accomplish the following tasks: (I) decrease the counterfeit production rate "$a\cdot$p" via the difficulty associated with anti-counterfeiting technologies, (II) decrease the fraction of successful pass attempts "s," (III) decrease the fraction of pass attempts that are detected but not reported "h," (IV) increase the fraction of pass attempts that are detected and reported "r," (V) increase the rate of the repass attempts in circulation "θ," and (VI) increase the rate of culling by the central bank "β." However, task (V) means increasing damage by counterfeit smart-banknotes, and the effects of task (VI) are ignored since the rate of culling is beyond the viewpoint of technological impact. Task (IV) is synonymous with tasks (II) and (III) since "$1 = h + r + s$"; therefore, it is important to decrease "s" and "h" as well as "$a\cdot$p."

To effectively analyze the smart-banknote system, parameters should be quantified. Although many parameters remain unknown, we can compare the parameters "s, h, a" before and after implementation of our system by referring to the results of FTA (see Section 4.2).

"a_i, r_i and h_i" are defined as the above parameters "a, r, h" corresponding to level of the counterfeiter, namely, index "i." Parameters with tilde, "$\tilde{a}_i$, $\tilde{r}_i$, $\tilde{h}_i$," are not affected by the smart-banknote system: parameters on the paper-based banknote system.

For low-level counterfeiters, the manufacturing volume is reduced according to "$a_{1,2,3}$," namely, difficulty associated with smart-banknote-anti-counterfeiting technology. From the results of FTA, we can estimate "$\tilde{a}_{1,2,3} \geq a_{1,2,3}$."

Even if they made counterfeit smart-banknotes, they cannot produce clone tags. Then the distinguish function works effectively. So we can estimate "$\tilde{s}_{1,2,3} \geq s_{1,2,3}$." If more and more people authenticate the smart-banknote by the smartphone, the parameter "$s_{1,2,3}$" approaches zero since counterfeits of this level are not possible to pass the verification of the distinguish function.

If a verifier, who finds counterfeits, uses them again, the amount of counterfeits in circulation will not be reduced. In the case of the proposed system, the verification results are reported to the data center by smartphones, and the fraction of pass attempts that are detected but not reported "$h_{1,2,3}$" tends to decrease. We can estimate "$\tilde{h}_{1,2,3} \geq h_{1,2,3}$."

The amount of low-level counterfeit smart-banknotes in circulation is given by the following.

$$\frac{(\tilde{s}_{1,2,3}+\tilde{h}_{1,2,3})\cdot(\tilde{a}_{1,2,3}\cdot \mathrm{p}-\mathrm{c})}{(1-\tilde{s}_{1,2,3}-\tilde{h}_{1,2,3})\cdot\theta+\beta} \geq \frac{(s_{1,2,3}+h_{1,2,3})\cdot(a_{1,2,3}\cdot \mathrm{p}-\mathrm{c})}{(1-s_{1,2,3}-h_{1,2,3})\cdot\theta+\beta} \tag{3}$$

In contrast, level-4 counterfeiters can produce clone tags; therefore, the difficulty associated with smart-banknote technology does not have enough effects on anti-counterfeiting. We can estimate "$\tilde{a}_4 \approx a_4$."

The distinguish function does not work effectively. On the other hand, under the assumption that a large number of smart-banknotes with the same tag/printed-serial-number are in circulation, the validity-checking function and the analytical function are effective. The fraction of successful pass attempts "s_4" tends to be decreased by the validity-checking function and the analytical function. We can estimate "$\tilde{s}_4 \geq s_4$."

The fraction of pass attempts that were detected but not reported "h_4" tends to decrease by reporting the verification results via smartphones ($\tilde{h}_4 \geq h_4$).

According to the above considerations, the amount of level-4 counterfeit smart-banknotes in circulation is given as

$$\frac{(\tilde{s}_4+\tilde{h}_4)\cdot(\tilde{a}_4\cdot \mathrm{p}-\mathrm{c})}{(1-\tilde{s}_4-\tilde{h}_4)\cdot\theta+\beta} \geq \frac{(s_4+h_4)\cdot(a_4\cdot \mathrm{p}-\mathrm{c})}{(1-s_4-h_4)\cdot\theta+\beta} \tag{4}$$

There are trivial results for Eqs. (3), (4). When "$(s_i + h_i) = 0$ or $a_i = 0$," our system is at its most effective. When "$(s_i + h_i) = 1$ and $a_i = 1$," our system is at its least effective.

From Eqs. (3), (4), we can see the followings.

In order to reduce the counterfeit smart-banknotes in circulation, it is important to reduce "s_i, h_i, a_i." The parameter "a_i" affects only the numerator of Eqs. (3), (4). On the other hand, the parameters "s_i and h_i" affect not only the numerator but also the denominator of Eqs. (3), (4).

In our proposal, we can expect that the parameters "s_i, h_i" become smaller than the previous ones. This is the effect of adding the ICT to conventional anti-counterfeit technologies.

5. Conclusion & Future Work

A "smart-banknote system," which authenticates banknotes by smartphone, was developed, and its effectiveness was evaluated by FTA. The evaluation shows that the smart-banknote system is most effective against low-level counterfeiters (level-3 or lower) and reasonably effective against level-4 counterfeiters.

Moreover, we proposed a new flow model for smart-banknotes. The amount of counterfeit smart-banknotes was evaluated using the flow model. With the aid of the flow model, we estimated the steady-state amount of unused counterfeit smart-banknotes in stockpile, "x(∞)," and the steady-state amount of counterfeits in circulation, "y(∞)." The evaluation shows that it is important to

decrease successful-pass attempt rate "s" and reuse rate "h" as well as manufacturing volume "$a \cdot$ p."

However, following topics were not yet studied, and they remain as targets for future work.

• Privacy Protection: in the proposed system, we send the verification results to the data center by the smartphone. Therefore, the data center might get the equipment identifier of sender's smartphone. Cooperating with the telecommunications carrier, the data center may be able to identify the sender using the equipment identifier. In this case, the datacenter can link "people," "place" and "time" since we send the verification results to the data center with the information of time and location. The data center might get the information of a payer and payee by tracking the printed-serial-number of banknotes. This could be a privacy risk because activity areas and friendship networks may be analyzed. Therefore, we may need two kinds of data center. One receives information from smartphones. Another analyzes the information without equipment identifiers. Then, the data centers cannot link "people," "place" and "time" unless these centers act in collusion.

There are other problems. By embedding an RFID-tag in banknotes, a stranger may scan the money in a wallet from outside. Therefore, we might need to adjust the effective range to a few centimeters from RFID tags, and/or we might use a wallet with radio shielding.

• Durability Requirement for the RFID-tag: in Section 1, we have introduced the durability of current chip. We assume that these data indicate sufficient durability in daily life use. However, the Bank of Japan has not disclosed the durability requirement for banknotes. Moreover, the durability requirement may vary across countries. Therefore, in cooperation with authorities in each country, we will need to define the conditions required for RFID-tags in the future.

• Operational Design for Smart-banknote: we have introduced the outline of this topic in Section 2.5. However, optimal operation varies across countries. We would like to investigate the condition of each country and to study the operational design for RFID-tag-embedded-banknote more deeply in future work.

• Social Acceptability: in particular, we think that social acceptability is mostly the problem on privacy protection. The proposed method for privacy protection is not necessarily accepted in every country. First of all, some people are reluctant to having RFID-tags embedded in banknotes. We think that a feeling of reluctance varies in each country. Therefore, we should investigate the national character and the social situation in each country. We need to build up as many successful cases as possible in some country based on investigation results.

• High Function Chip: recently, there is a topic called Physical Unclonable Function (PUF). Gassend et al. described silicon-based PUF [7]. A silicon-based PUF is a function that outputs a device-specific response by extracting its intrinsic physical characteristics such as particulate diffusion and microscopic variation of silicon devices. The physical characteristics of the devices are practically unclonable, and therefore a PUF is expected to output unique responses used for device authentication. The PUF component has been implemented in less than 0.02 mm^2 [8]. PUF-enabled RFIDs are expected to be embedded in smart-banknotes in the future. We would like to evaluate the smart-banknotes with PUF-enabled tags in our future work.

References

[1] A Path to the Next Generation of U.S. Banknotes: Keeping Them Real, National Research Council, National Academies Press (2007).

[2] Gergen, B., Nienhaus, H., Weinberg, W.H. and McFarland, E.W.: Chemically Induced Electronic Excitations at Metal Surfaces, *Science*, Vol.294, pp.2521–2523 (2001).

[3] Chen, Y., Mihcak, M.K. and Kirovski, D.: Certifying Authenticity via Fiber-Infused Paper, *ACM SIGecom Exchanges*, Vol.5, No.3, pp.29–37 (2005).

[4] Reuss, R., Chalamala, B.R., Moussessian, A., Kane, M.G., Kumar, A., Zhang, D.C., Rogers, J.A., Hatalis, M., Temple, D., Moddel, G., Eliasson, B.J., Estes, M.J., Kunze, J., Handy, E.S., Harmon, E.S., Salzman, D.B., Woodall, J.M., Alam, A.A., Murthy, J.Y., Jacobsen, S.C., Olivier, M., Markus, D., Campbell, P.M. and Snow, E.: Macroelectronics: Perspectives on technology and applications, *Proc. IEEE*, Vol.93, No.7, pp.1239–1256 (2005).

[5] Marinov, V.R., Swenson, O., Miller, R., Sarwar, F., Atanasov, Y., Semler, M. and Datta, S.: Laser-Enabled Advanced Packaging of Ultrathin Bare Dice in Flexible Substrates, *IEEE Trans. Components, Packaging and Manufacturing Technology*, Vol.2, No.4, pp.569–577 (2012).

[6] Marinov, R., Swenson, O., Atanasov, Y. and Schneck, N.: Laser-assisted ultrathin bare die packaging: A route to a new class of microelectronic devices, *Proc. SPIE*, Vol.8608, 86080L (2013).

[7] Gassend, B., Clarke, D., van Dijk, M. and Devadas, S.: Silicon physical random functions, *Proc. 9th ACM Conference on Computer and Communications Security*, pp.148–160, ACM Press (2002).

[8] Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T. and Khandelwal, V.: Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications, *RFID 2008 IEEE International Conference*, pp.58–64 (2008).

[9] National Police Agency: The Number of Counterfeits Discovered, available from ⟨http://www.npa.go.jp/toukei/souni/gizou.xls⟩ (accessed 2013-01).

[10] The Federal Reserve Board: The Use and Counterfeiting of United States Currency Abroad, Part3, available from ⟨http://www.federalreserve.gov/boarddocs/rptcongress/counterfeit/counterfeit2006.pdf⟩ (accessed 2013-01).

[11] European Central Bank: Biannual information on euro banknote counterfeiting, available from ⟨http://www.ecb.int/press/pr/date/2012/html/index.en.html⟩ (accessed 2013-01).

[12] Bank of England: Counterfeit Bank of England banknotes available from ⟨http://www.bankofengland.co.uk/banknotes/Pages/about/counterfeits.aspx⟩ (accessed 2013-01).

[13] Banco Central do Brasil: Falsificação de Cédulas, available from ⟨http://www.bcb.gov.br/?MECIRESTFALSAS⟩ (accessed 2013-01).

[14] Reserve Bank of India: AnnualReport CURRENCY MANAGEMENT, available from ⟨http://www.rbi.org.in/scripts/AnnualReportPublications.aspx?Id=1045⟩ (accessed 2013-01).

[15] The Federal Reserve Board: Value of currency in circulation, available from ⟨http://www.federalreserve.gov/paymentsystems/files/coin_currcircvalue.pdf⟩ (accessed 2013-01).

[16] NFC Forum, available from ⟨http://www.nfc-forum.org/home/⟩ (accessed 2013-01).

[17] MF0ICU2 MIFARE Ultralight C, NXP, 2009, available from ⟨http://www.nxp.com/documents/short_data_sheet/MF0ICU2_SDS.pdf⟩ (accessed 2013-01).

[18] NTAG213/215/216, NXP, 2013, available from ⟨http://www.nxp.com/documents/data_sheet/NTAG213_215_216.pdf⟩ (accessed 2015-03).

[19] 2012-2013 nen-ban smartphone/tablet no global shijo-tenbou (in Japanese) [Global market forecast of smartphone/tablet, 2012-2013], Seed Planning, Inc. (2012).

[20] Sekai no NFC shijo-senryaku 2010 (in Japanese) [NFC market strategy in the world, 2010], Seed Planning, Inc. (2010).

[21] Japan patent JP2005-350823

[22] CQ Publishing Co., Ltd., 0.4 mm-kaku RFID-chip ⌈μ-chip⌋ no sekkeigijutu (Japanese) [Design of 0.4 mm^2 RFID chip: μ-chip]: *Design Wave Magazine*, pp.129–130 (2003), available from ⟨http://www.cqpub.co.jp/dwm/contents/0068/dwm006801290.pdf⟩ (accessed 2015-03).

[23] Hornyak, T.: RFID Powder, *Scientific American*, pp.68–71 (2008). available from ⟨http://www.cs.virginia.edu/~robins/RFID_Powder.pdf⟩ (accessed 2015-03).

[24] Usami, M., Tanabe, H., Sato, A., Sakama, I., Maki, Y., Iwamatsu,

T., Ipposhi, T. and Inoue, Y.: A 0.05x0.05 mm^2 RFID Chip with Easily Scaled-Down ID-Memory, ISSCC Digest of Technical Papers, pp.482–483 (2007).
[25] Renesas Electronics Corporation: RKT102***MH, Precautions and Notes in Connection with Mounting COA-Type μ-Chip Inlet (2007). available from ⟨http://documentation.renesas.com/doc/products/rfid/rej11p0007_rkt102_mhum.pdf⟩ (accessed 2015-03).
[26] Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), ANSI, ANSI X9.62-1998 (1998).
[27] SEC2: Recommended Elliptic Cureve Domain Parameters, The Standards for Efficient Cryptography, available from ⟨www.secg.org/download/aid-784/sec2-v2.pdf⟩ (accessed 2013-01).
[28] Institute for Monetary and Economic StudiesBank of Japan: Functions and Operations of the Bank of Japan, (2012). available from ⟨http://www.boj.or.jp/en/about/outline/data/fobojall.pdf⟩ (accessed 2015-03).
[29] Exchange of Bank of Japan Notes, Article 48 of Bank of Japan Act
[30] Shin-shihei, Iron-gake Chuui (Japanese) [Refrain from Ironing to New-banknote], The Asahi Simbun Company, newspaper article, p.39 (Saturday 2004-11-27).

Hisao Sakazaki received his B.S. and M.S. degrees in mathematics from Kanazawa University, Japan, in 1994 and 1996, respectively, and Ph.D. degree in information science from Japan Advanced Institute of Science and Technology (JAIST), in 1999. Since 1999, he has worked in the field of information security at Research & Development Group of Hitachi, Ltd., Japan.

Yasuko Fukuzawa received her B.E. degrees in physics from Japan Women's University, in 1985, and Ph.D. degree in engineering from Yokohama National University, in 2007. Since 1985, she has worked in the field of information security at Research & Development Group of Hitachi, Ltd., Japan.