Security Analysis of Offline E-cash Systems with Malicious Insider *†

Takashi Nishide‡
Kyushu University
Fukuoka, Japan
nishide@inf.kyushu-u.ac.jp

Shingo Miyazaki
Toshiba Solutions
Tokyo, Japan
Miyazaki.Shingo@toshiba-sol.co.jp

Kouichi Sakurai
Kyushu University
Fukuoka, Japan
sakurai@inf.kyushu-u.ac.jp

Abstract

When we build electronic cash systems, the main focus of the design is usually on preventing customers' malicious actions. However, since authorities such as banks and certificate authorities may have important secret data of customers, the insiders in the potentially untrusted authorities can become threats to electronic cash systems. Miyazaki and Sakurai [2] first systematically analyzed security of offline anonymous electronic cash systems by considering the insider threats from untrusted authorities. They investigated the security of the existing electronic cash systems and categorized the systems into four types. In this paper, we reconsider the security of offline anonymous electronic cash systems including more recent systems based on the classification of Miyazaki and Sakurai and investigate the possible effective countermeasures against malicious insiders.

Keywords: Chaum-Fiat-Naor paradigm, double spending, electronic cash system, framing attack by bank, insider threat

1 Introduction

The research of electronic cash has long history and has been one of the important challenging problems in cryptography. Chaum proposed an online anonymous electronic cash system [3] by using blind signatures. In the system proposed by Chaum [3], the bank needs to be involved in the payment in order to

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 3, number: 1/2, pp. 55-71

*This paper is an extended version of the work originally presented at the 3rd International Workshop on Managing Insider Security Threats (MIST'11), Fukuoka, Japan, December 2011 [1]. This version does further investigation of the countermeasures against malicious insiders and includes more examples of potential insider attacks.

†This work is partly supported by Grants-in-Aid for Scientific Research (B) (23300027), Japan Society for the Promotion of Science (JSPS).

‡Corresponding author: Kyushu University, 744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan, Tel: +81-92-802-3666, Email: nishide@inf.kyushu-u.ac.jp, Web: http://itslab.inf.kyushu-u.ac.jp/~nishide/index.html

prevent double spending of electronic cash. The fact that the bank needs to be online for all the payment transactions between a customer and a shop can lead to the bottleneck of the bank system and it prevents realizing practical electronic cash systems.

Chaum, Fiat, and Naor proposed an offline anonymous electronic cash system [4] where the bank does not need to be involved in the payment transaction between a customer and a shop. Many electronic cash systems [5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33] follow the Chaum-Fiat-Naor approach (CFN paradigm). In the CFN paradigm, a customer withdraws electronic cash (e-cash) from the bank and sends the e-cash to a shop without needing to access the bank system. If the customer spends the e-cash only once, the anonymity of the customer is guaranteed. However, if the customer double-spends the e-cash maliciously, the bank can extract the identification information of the customer from the double-spent e-cash.

In the CFN paradigm, to realize both the offline property and the detection of double spending, the identification information of a customer is embedded in e-cash and also maintained by authorities such as banks. Such important identification information needs to be protected so that no malicious persons including bank employees can misuse it.

In many of the existing electronic cash systems, the banks and other third authorities are assumed to be trustworthy, and the insider attacks by untrusted authorities are not paid attention to. However, some of the bank employees may become malicious, for example, due to bribes and the internal secret data leakage may occur because of the vulnerabilities in bank software systems. Therefore, it is important to evaluate security of electronic cash systems in terms of the insider attacks by untrusted authorities if electronic cash systems are deployed in the real world. For example, Ferguson [10] mentioned the framing attack by a malicious bank and to prevent such an insider attack, Ferguson's approach is to sign the data exchanged at the withdrawal protocol. Though Ferguson's approach seems general, both the customer and the bank need to keep much data for a long time to avoid disputes.

In this paper, we reconsider the work [2] done by Miyazaki and Sakurai that first systematically analyzed the security of existing electronic cash systems against insider threats. Following the classification of Miyazaki and Sakurai, we investigate some of the recently proposed electronic cash systems [8, 9, 11, 12, 13, 14, 34] and analyze the promising approach of Hanatani el al. [9] and mention the countermeasures based on the non-cryptographic techniques.

1.1 Chaum-Fiat-Naor Paradigm for Offline Anonymous Electronic Cash

In the classification by Miyazaki and Sakurai [2], the electronic cash systems following the Chaum-Fiat-Naor (CFN) Paradigm [4] were analyzed, so we describe the CFN paradigm in more detail. A bank $\mathcal{B}$ has a pair of public and private keys $P_{\mathcal{B}}, S_{\mathcal{B}}$. A signature generated by using $S_{\mathcal{B}}$ can be considered to be e-cash corresponding to a certain amount of money w. In order to guarantee anonymity of customers, $\mathcal{B}$ generates this signature by using a blind signature technique. A customer C and a shop $\mathcal{S}$ have each bank account in the bank $\mathcal{B}$. In the electronic cash system, we have the following four protocols (See Fig. 1).

Withdrawal Protocol:

(i) A customer C generates a message m_C by using its own identification information S_C. C proves to $\mathcal{B}$ that C generated m_C correctly without revealing S_C.

(ii) $\mathcal{B}$ generates a signature on m_C by using a blind signature and withdraws money corresponding to w from the bank account of C.

(iii) C computes $\sigma_{\mathcal{B}}(m_C)$ as the $\mathcal{B}$'s signature on m_C.

Payment Protocol:

(i) C sends $(m_C, \sigma_{\mathcal{B}}(m_C))$ to a shop $\mathcal{S}$.

(ii) $\mathcal{S}$ verifies the signature $\sigma_{\mathcal{B}}(m_C)$ and if $\sigma_{\mathcal{B}}(m_C)$ is correct, $\mathcal{S}$ sends a random challenge $c_{\mathcal{S}}$ to C.

(iii) C computes and sends the response r_C to $\mathcal{S}$.

(iv) $\mathcal{S}$ verifies r_C and if it is correct, $\mathcal{S}$ exchanges goods and the e-cash with r_C.

Deposit Protocol:

(i) $\mathcal{S}$ sends $(m_C, \sigma_{\mathcal{B}}(m_C), c_{\mathcal{S}}, r_C)$ to the bank $\mathcal{B}$.

(ii) $\mathcal{B}$ verifies the bank's signature $(m_C, \sigma_{\mathcal{B}}(m_C))$ and a pair of the challenge and response $(c_{\mathcal{S}}, r_C)$. $\mathcal{B}$ stores $(m_C, \sigma_{\mathcal{B}}(m_C), c_{\mathcal{S}}, r_C)$ in the database for future detection of double spending and credits w to the bank account of $\mathcal{S}$.

Identification of Double-Spender:

(i) If a certain e-cash is double-spent, $\mathcal{B}$ extracts the identification information S_C of the double-spender from the two history data $(c_{\mathcal{S}}, r_C)$ and $(c'_{\mathcal{S}}, r'_C)$.

2 Possible Threats from Malicious Insiders

2.1 Impersonation

One of possible insider attacks by malicious banks (or malicious bank employees) is impersonation. For instance, in the system proposed by Chaum, Fiat, and Naor [4], the customer's secret key is stored in the database of the bank and in this case, the customer's ID is the secret key. This means a malicious bank employee may be able to steal the secret key of an honest customer. Therefore, the malicious bank employee can withdraw e-cash from the honest customer's account by impersonating the customer with the secret key (i.e., the customer's ID in this case), and what is worse, the malicious bank employee can double-spend the e-cash without compromising him/herself. If the secret key itself is stored in the database of the bank, this insider attack is difficult to prevent.

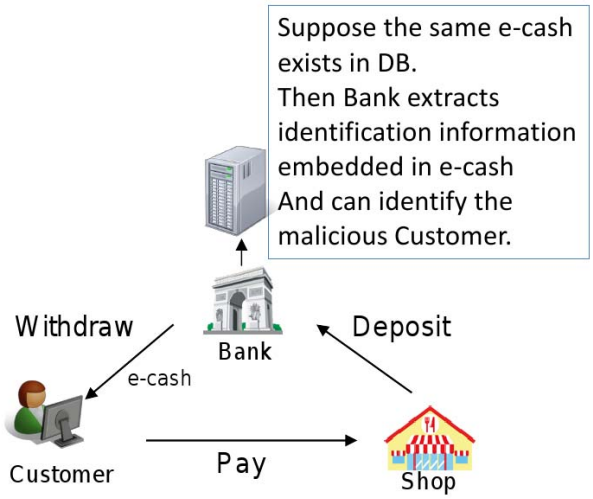


Figure 1: Basic Information Flow in Electronic Cash System

2.2 Framing Attack

In the framing attack, a malicious bank forges facts of double spending. In the systems [24, 5, 6, 28, 19, 10, 16, 27, 31, 15], ElGamal signatures and Okamoto-Schnorr signatures in the payment are used to identify double-spenders and a malicious bank can misuse these signatures to forge a fact of double spending as follows.

Now let U be the secret key of a customer and let k be the random value chosen by the customer in the withdrawal and let m be the random challenge chosen by a shop. If the customer double-spends an e-cash, the bank computes U and k by using the equations

$$r_1 = Um_1 + k, \quad r_2 = Um_2 + k,$$

and identifies the double-spender with U. Then the malicious bank can generate another signature $r_3 = Um_3 + k$ by using U and a new random challenge m_3. This means that the malicious bank can forge a new fact of double spending by showing the signatures r_1, r_2, r_3 and this can be problematic because the first double spending might be caused unintentionally due to software flaw or computer viruses, etc.

In Schoenmakers' scheme [31], the bank knows U and even if the customer does not double-spend the e-cash, the bank can forge a fact of the honest customer's double spending by colluding with a shop as follows.

Step 1: The bank colludes with a shop. When the shop sends the e-cash to the bank for the deposit, the bank knows the customer (U) that spent the e-cash. Let $r = Um + k$ be the signature in the payment (actually this is a simplified explanation).

Step 2: The bank computes the random value chosen by the customer k from r, U, m.

Step 3: The bank computes a fake signature $r' = Um' + k$ from fake random challenge m'.

Step 4: The bank claims that the customer double-spent the e-cash by showing the two signatures r, r'.

Though the malicious bank needs to collude with a shop to revoke the anonymity, the bank can make the framing attack even on the honest customer.

In the Yacobi's scheme [15], the ElGamal signature is used similarly, but the bank cannot make the same attack on an honest customer because the bank does not know the customer's secret key. However, the bank can make the framing attack on the double-spender more than twice illegally.

2.3 Collusion between Bank and Shop

In the systems of [17, 16, 18, 15], a customer uses the same signing key and public key certificate in every payment. In this case, a shop can distinguish customers, so it may be able to associate the identification information of a customer with the public key certificate. Therefore, if the bank and the shop collude, the bank can know the purchase history of a customer by checking the public (verification) key of the e-cash in the deposit and the anonymity of the customer can be broken. This happens because the same keys are used in every payment. In the system proposed by Peterson and Poupard [21], the anonymity of a customer is strengthened by using multiple different keys in the payment.

3 Classification of Offline Electronic Cash Systems

3.1 Offline Electronic Cash System and Secret Key

In offline electronic cash systems, the identification of a double-spender is based on the communication data during the payment protocol. Typically, if an e-cash is double-spent, the identification information of the double-spender is extracted from the e-cash. In some other systems, the customer C generates a signature on the random challenge sent by the shop $\mathcal{S}$ and the double-spender is identified by extracting the signing key. In the classification defined by Miyazaki and Sakurai [2], such identification information and signing keys to identify double-spenders are treated as *secret keys*. These secret keys can be misused by untrusted authorities for impersonation of customers, forgery of the facts of double spending, etc and cause insider threats.

3.2 Classification

The classification by Miyazaki and Sakurai [2] is based on what kind of information about customers' secret keys the authorities store in their databases (See Fig. 2).

Type I:

The customer's secret key itself is directly stored in the database of a bank as the identification information and embedded in the withdrawn e-cash.

An adversary can impersonate the customer easily if he obtains the identification information of the customer stored in the database. The systems of Type I^+ are more secure than the systems of

Type I and in such systems, the customer has another secret key for signing the communication data with the bank, which prevents the bank's framing attack [10].

Type II:

The customer's public key is stored in the database of a bank as the identification information while the corresponding secret key is known only to the customer. This type has no certificate on the customer's public key.

In the systems of Type II such as Brands' [5], the customer's public key is registered as the customer's identification information and it is embedded in the withdrawn e-cash by the bank. An adversary can impersonate the customer if he can obtain the secret key corresponding to the public key stored in the database of the bank.

Type III:

The customer registers his public key as his identification information and makes payments with the key and the certificate for the public key. For an adversary to impersonate the customer, he needs to obtain the forged certificate in addition to extracting the corresponding secret key from the public key.

Performing the impersonation in the systems of Type III$^+$ is more difficult than in Type III. For Type III$^+$, the adversary has a more difficulty connecting the public key to its owner in the database of authorities.

Type IV:

The secret key consists of two parts. One is known both to the authority and to the customer while the other is computed only by the customer. The corresponding public key and its certificate are known only to the customer.

In the systems of Type IV, the customer's identification information stored in the (trusted) authority (e.g., bank) can produce little knowledge of the corresponding secret key. Therefore, this incomplete information (for the bank) enhances security against the impersonation by the malicious bank.

As a general rule, Type IV can be considered to be the most secure because the information given to the insiders is very limited and it makes the insider attacks more difficult.

3.3 Security of Type IV

We consider the e-cash systems [15, 6, 16] that belong to Type IV.

In the system proposed by Brands [6], a tamper-proof device was introduced to store the identification information of a customer that is known only to the bank. The bank offers this tamper-proof device to the customer. The customer's secret key consists of (s_1, s_2) where s_1 stored in the tamper-proof device

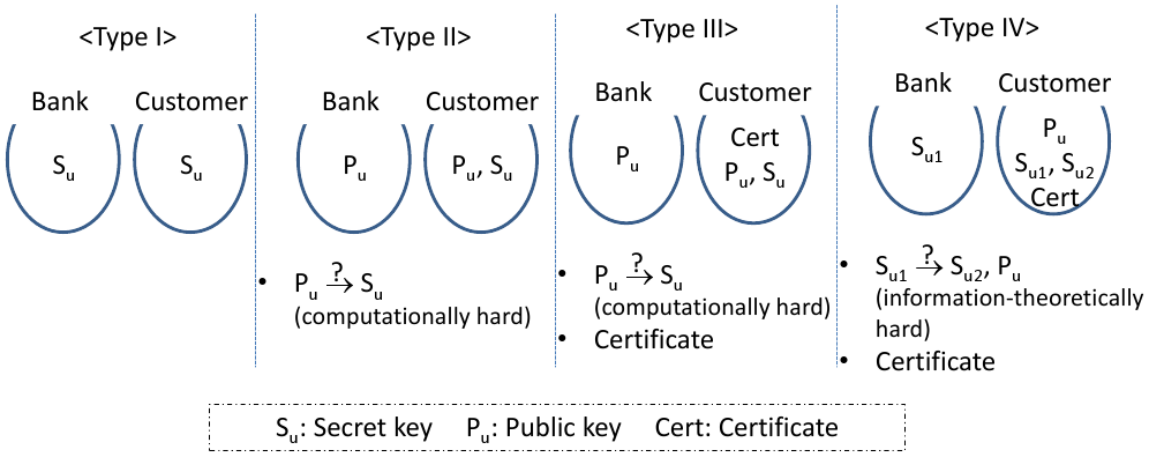


Figure 2: Customer Information Stored in Bank Database and Customer [2]

is known only to the bank and s_2 is known only to the customer. In this case, the tamper-proof device is considered to be a kind of a trusted third party or an unforgeable certificate. The security of the Brands' system [6] heavily relies on the tamper-proofness. If the physical verification of the authenticity of the tamper-proof device does not hold, the type of the Brands' system [6] falls into Type II.

In the systems proposed by Yacobi [15] and Miyazaki and Sakurai [16], a certificate authority (CA) exists and it issues a certificate for a customer's secret key where the secret key S consists of the identification information (ID) and a secret random number R (i.e., $S = ID||R$). If the CA is malicious, the CA can impersonate a customer ID by issuing a certificate for a secret key $S' = ID||R'$ where ID is public information and R' can be chosen freely by the malicious CA itself. One possible countermeasure is to have multiple CAs and distribute the functionality of issuing certificates among them.

4 Recently Proposed Systems

Blazy et al. [14] investigated offline transferability. The property called offline transferability means that the recipient of an e-cash can transfer it to another person without contacting any authority. In the Blazy et al.'s system [14], a trusted authority called judge is introduced and the judge can extract the identity of a double-spender after the bank detects the double spending. A customer generates its own pair of public and private keys and obtains a certificate from the judge. Therefore, the system of Blazy et al. [14] is classified as Type III.

Canard et al. [12] also discussed how to realize efficient transferable e-cash, and the system is based on the protocol of Camenisch, Hohenberger, and Lysyanskaya [35]. In the system proposed by Canard et al. [12], the public key of a customer needs to be known to the bank, and the customer obtains the certificate from the bank, so it is classified as Type III.

Canard et al. [11] defined two levels of anonymity called full anonymity and perfect anonymity in the transferable e-cash setting rigorously. Full anonymity means that an adversary cannot recognize

the e-cash he has already observed during a payment protocol between honest customers, and perfect anonymity means that the adversary cannot decide whether or not he has already owned the e-cash he is receiving. The system proposed by Canard et al. [11] follows the design principle of their previous work [12] and it is classified as Type III.

Canard et al. [13] considered a divisible e-cash system in which e-cash can be divided into multiple denominations in the payment protocol. They use the binary tree of keys and improve the drawback of Au et al.'s system [36]. In the system proposed by Canard et al. [13], it is assumed that any user public key is certified by an authority and the bank can be convinced that the customer is already registered in the system. Therefore, the system proposed by Canard et al. [13] is classified as Type III.

Au et al. [34] considered anonymous customer suspension by introducing a new entity called suspension manager. The suspended customer cannot perform new transactions and if the customer turns out to be innocent later, the customer can be unsuspended without breaching anonymity. In the system proposed by Au et al. [34], the public key of a customer needs to be known to the bank, so it is classified as Type II.

We summarize the types of existing e-cash systems in Table 1 including the classification done by Miyazaki and Sakurai [2]. Note that the classification of some systems depends on the settings where they are deployed. Here `Key Management Center` (`Key M. C.`) means the name of an organization with which the customer's information (e.g., the secret key, the public key, etc) is deposited. Some systems discuss how to cope with criminal attacks such as money laundering and blackmailing [37]. In order to resist these criminal attacks, we usually need a special functionality to deanonymize e-cash even if it is not double-spent.

5 Countermeasure Against Insider Threats

As mentioned by Miyazaki and Sakurai [2], one possible effective way is to distribute important functionalities among multiple authorities. For instance, in the distributed certificate authority, a threshold signature scheme is used and the certificate can be issued only when at least the threshold number of authorities agree on that. By requiring authorities to obtain an agreement from other authorities, we are more likely to be able to deter insider attacks by malicious authorities.

5.1 Hanatani et al.'s E-cash System

One of the elegant solutions to insider attacks by malicious banks was proposed by Hanatani et al. [8, 9]. Hanatani et al. use a blind multisignature scheme based on the Abe's scheme [38] instead of a threshold signature scheme (e.g., Shoup's threshold signature [39]). In the system proposed by Hanatani et al. [9], an e-cash needs to be signed by multiple banks specified by the customer and also the e-cash needs to include a signature by the customer. Therefore, the e-cash cannot be created without an agreement from the customer and this mechanism prevents malicious banks from framing the customer by creating a non-agreed e-cash and forging the fact of double spending.

Also in the system proposed by Hanatani et al. [9], the public key of a customer is known to anyone,

Table 1: Classification of offline e-cash systems

System	Type	Key M. C.	Criminal Atk.	Notes
CFN88 [4]	I	Bank	No	The first offline e-cash system
FY93 [30]	I	Bank	No	Provable Security Argument
Sch95 [31]	I^+	Bank	No	Scheme withstanding parallel attacks
$BGK95_\beta$ [24]	I	Bank	Discussed	Franklin-Yung based ([33])
JY96 [32]	III, II, or I	Bank	Discussed	Resistant against bank robberies attacks
Pai92 [29]	I^+	Bank	No	Based on Guillou-Quisquater scheme
Fer93 [10]	I^+	Bank	No	Discussion on framing by a malicious bank
ASM11 [34]	II	Bank	No	Anonymous customer suspension
Bra93 [5]	II	Bank	No	Based on the technique of restrictive blinding
DdC94 [23]	II	Public File	No	Transferable e-cash without any increase in size
$BGK95_\alpha$ [24]	II	Bank	Discussed	Brands-based ([5])
CMS96 [25]	II	Bank	Discussed	Passive anonymity-revoking trustee
FTY96 [26]	II	Bank	Discussed	Anonymity-revoking via ElGamal decryption
NMV97 [27]	II	Bank	No	Based on Nyberg-Rueppel signature
dST98 [28]	II	Bank	Discussed	Based on modified restrictive bliding scheme
BCFGST11 [14]	III	Bank	No	Transferable e-cash with Groth-Sahai proofs
CGT08 [12]	III	Bank	No	Transferable e-cash w/ unconditional anonymity
CG08 [11]	III	Bank	No	Transferable e-cash w/ full/perfect anonymity
CG10 [13]	III	Bank	No	Multiple denominations in e-cash
OO91 [18]	III	Bank	No	The first divisible e-cash
EO94 [19]	III	Bank	No	Single-term divisible e-cash
Oka95 [20]	III	Bank	No	Improving efficiency of scheme [19]
PP97 [21]	III	TTP	Discussed	Extortion-tracing under offline payment
MAFN97 [22]	III	RC	No	Central institution issuing e-cash for other banks
HKOK07 [9]	III	PKI	No	Keys of customers and banks are based on PKI
FO96 [17]	III^+	TTPs	Discussed	Anonymous channels or distributed structure
Yac94 [15]	IV	CA,Bank	No	GMR-ZKP at initial certificate and withdrawal
Bra95 [6]	IV ($\rightarrow$ II)	TPD, Bank	No	Tamper-proof device managing ID of customer
MS98 [16]	IV	RC	No	Partially blind signature based on DLP

TTP: Trusted Third Party, RC: Registration Center, PKI: Public Key Infrastructure,
CA: Certificate Authority, TPD: Tamper-Proof Device, DLP: Discrete Log Problem,
GMR-ZKP: Goldwasser-Micali-Rackoff Zero-Knowledge Proof

so it is classified as Type III. However, the private (secret) key of the customer is not revealed even when the double spending is detected. That is, only the identity (public key) of the customer is extracted from

the double-spent e-cash. Therefore, the malicious banks cannot impersonate the customer, and an ideal setting for preventing the insider attacks is realized. This design principle is very important. For example, in the Brands' system [5], a customer generates a pair of public key and private key such that the public key is $I = g_1^U$ and the private key is U. The bank stores the customer's public key I in the database of the bank. If an e-cash is double-spent, the bank can extract, from the double-spent e-cash, the private key U of the double-spender rather than the public key I. Then the bank can abuse the customer's private key for impersonation, and furthermore can frame the customer by making another fact of double spending. However, the private key itself is not extracted in the system of Hanatani et al. [9], and the insider attacks can be prevented successfully.

Hanatani et al. [9] defined a new security model including blind multisignatures and multiple banks and provided a rigorous security analysis. More precisely, Hanatani et al. defined the following security requirements and gave the security proofs based on these.

Adaptive Chosen Message Attack

An adversary can request an arbitrary set of banks to issue e-cash.

Adaptive Insider Attack

An adversary can corrupt an arbitrary set of banks except a bank that is an attack target.

Untraceability to Honest Customer

No honest customer's anonymity should be breached.

Traceability to Dishonest Customer

If an e-cash is double-spent, the dishonest customer (double-spender) should be identified.

One-more Unforgeability of E-cash

No customer should be able to obtain $\ell + 1$ e-cash from ℓ e-cash.

Unissuability without Customer's Permission

No banks should be able to issue a customer's e-cash without the customer's agreement.

We can see that "Unissuability without Customer's Permission" actually captures the most important requirement in terms of insider threats and this requirement will always need to be considered when we build a new e-cash system that is resistant against insider threats.

5.2 Countermeasures based on Non-Cryptographic Techniques

Many of the insider threats in e-cash systems come from malicious data theft. Recently there are several approaches to detecting malicious insiders' actions including insider data theft such as the methods of Bowen et al. [40] and Grier [41]. For example, Bowen et al. [40] introduced decoy data to deceive malicious insiders, and the proposed method can signal an alert when the decoy data is accessed. Grier [41] proposed how to detect data copy operations that can lead to malicious disclosure of secret information by monitoring the filesystem activities.

Furthermore there is a DARPA project called "Proactive Discovery of Insider Threats Using Graph Analysis and Learning" (that is part of the project "Anomaly Detection at Multiple Scales"). In this kind of approaches, unusual activities by insiders (i.e., employees in an organization) are predicted by using various techniques such as machine learning and anomaly detection.

These techniques will be applicable to deterring potential malicious insiders from stealing and misusing secret information.

6 Concluding Remark

In the research of offline e-cash systems, often the insider threats from untrusted authorities are not paid attention to. Miyazaki and Sakurai [2] first pointed out that the systematic study of the insider attacks against offline e-cash systems based on the CFN paradigm was insufficient and gave a classification useful for security evaluation. Careful consideration to the insider threats will need to be taken for offline e-cash systems to be truly practical. Other countermeasures against the insider threats such as audit and logging will also need to be deployed with forensics techniques.

Hanatani et al. gave an elegant solution to resist an insider attack from a malicious bank. Potential future work will include adding a functionality for deanonymization to Hanatani et al. [9] to deal with criminal attacks such as money laundering and blackmailing [37].

Digital Rights Management (DRM) may be considered to be one of potential applications of the e-cash technology [42] and double spending detection of the e-cash technology will be useful for realizing copy and access control mechanisms with privacy protection.

References

[1] T. Nishide and K. Sakurai, "Security of offline anonymous electronic cash systems against insider attacks by untrusted authorities revisited," in *Proc. of the 3rd International Conference on Intelligent Networking and Collaborative Systems (INCoS'11), Fukuoka, Japan*. IEEE, November 2011, pp. 656–661.

[2] S. Miyazaki and K. Sakurai, "Classification of chaum-fiat-naor paradigm based anonymous electronic cash systems according to vulnerability against insider-attacks from untrusted authorites," in *Cryptographic Techniques and E-Commerce, Hong Kong*, M. Blum and C. H. Lee, Eds. City University of Hong Kong Press, July 1999, pp. 262–271.

[3] D. Chaum, "Blind signatures for untraceable payments," in *Proc. of Advances in Cryptology (CRYPTO'82), Santa Barbara, California, USA*. Plenum Press, New York, August 1982, pp. 199–203.

[4] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in *Proc. of the 8th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'88), Santa Barbara, California, USA, LNCS*, vol. 403. Springer-Verlag, August 1988, pp. 319–327.

[5] S. Brands, "Untraceable off-line cash in wallets with observers (extended abstract)," in *Proc. of the 13th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'93), Santa Barbara, California, USA, LNCS*, vol. 773. Springer-Verlag, August 1993, pp. 302–318.

[6] ——, "Off-line electronic cash based on secret-key certificates," in *Proc. of Theoretical Informatics, Second Latin American Symposium (LATIN'95), Valparaíso, Chile, LNCS*, vol. 911. Springer-Verlag, April 1995, pp. 131–166.

[7] A. H. Chan, Y. Frankel, P. D. MacKenzie, and Y. Tsiounis, "Mis-representation of identities in e-cash schemes and how to prevent it," in *Proc. of International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT'96), Kyongju, Korea, LNCS*, vol. 1163. Springer-Verlag, November 1996, pp. 276–285.

[8] Y. Hanatani, Y. Komano, K. Ohta, and N. Kunihiro, "Provably secure electronic cash based on blind multisignature schemes," in *Proc. of the 10th International Conference on Financial Cryptography and Data Security (FC'06), Anguilla, British West Indies, LNCS*, vol. 4107. Springer-Verlag, February 2006, pp. 236–250.

[9] ——, "Provably secure untraceable electronic cash against insider attacks," *IEICE Transactions*, vol. 90-A, no. 5, pp. 980–991, May 2007.

[10] N. Ferguson, "Single term off-line coins," in *Proc. of Workshop on the Theory and Application of of Cryptographic Techniques (EUROCRYPT'93), Lofthus, Norway, LNCS*, vol. 765. Springer-Verlag, May 1993, pp. 318–328.

[11] S. Canard and A. Gouget, "Anonymity in transferable e-cash," in *Proc. of the 6th International Conference on Applied Cryptography and Network Security (ACNS'08), New York, NY, USA, LNCS*, vol. 5037. Springer-Verlag, June 2008, pp. 207–223.

[12] S. Canard, A. Gouget, and J. Traoré, "Improvement of efficiency in (unconditional) anonymous transferable e-cash," in *Proc. of the 12th International Conference on Financial Cryptography and Data Security (FC'08), Cozumel, Mexico, LNCS*, vol. 5143. Springer-Verlag, January 2008, pp. 202–214.

[13] S. Canard and A. Gouget, "Multiple denominations in e-cash with compact transaction data," in *Proc. of the 14th International Conference on Financial Cryptography and Data Security (FC'10), Tenerife, Canary Islands, LNCS*, vol. 6052. Springer-Verlag, January 2010, pp. 82–97.

[14] O. Blazy, S. Canard, G. Fuchsbauer, A. Gouget, H. Sibert, and J. Traoré, "Achieving optimal anonymity in transferable e-cash with a judge," in *Proc. of the 4th International Conference on Cryptology in Africa (AFRICACRYPT'11), Dakar, Senegal, LNCS*, vol. 6737. Springer-Verlag, July 2011, pp. 206–223.

[15] Y. Yacobi, "Efficient electronic money (extended abstract)," in *Proc. of the 4th International Conference on the Theory and Applications of Cryptology (ASIACRYPT'94), Wollongong, Australia, LNCS*, vol. 917. Springer-Verlag, November 1994, pp. 153–163.

[16] S. Miyazaki and K. Sakurai, "A more efficient untraceable e-cash system with partially blind signatures based on the discrete logarithm problem," in *Proc. of the 2nd International Conference on Financial Cryptography (FC'98), Anguilla, British West Indies, LNCS*, vol. 1465. Springer-Verlag, February 1998, pp. 296–308.

[17] E. Fujisaki and T. Okamoto, "Practical escrow cash system," in *Proc. of 1996 International Workshop on Security Protocols, Cambridge, United Kingdom*, vol. 1189. Springer-Verlag, April 1996, pp. 33–48.

[18] T. Okamoto and K. Ohta, "Universal electronic cash," in *Proc. of the 11th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'91), Santa Barbara, California, USA, LNCS*, vol. 576. Springer-Verlag, August 1991, pp. 324–337.

[19] T. Eng and T. Okamoto, "Single-term divisible electronic coins," in *Proc. of Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT'94), Perugia, Italy, LNCS*, vol. 950. Springer-Verlag, May 1994, pp. 306–319.

[20] T. Okamoto, "An efficient divisible electronic cash scheme," in *Proc. of the 15th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'95), Santa Barbara, California, USA, LNCS*, vol.

963. Springer-Verlag, August 1995, pp. 438–451.

[21] H. Peterson and G. Poupard, "Efficient scalable fair cash with off-line extortion prevention," in *Proc. of the 1st International Conference on Information and Communications Security (ICIS'97), Beijing, China, LNCS*, vol. 1334. Springer-Verlag, November 1997, pp. 463–477.

[22] H. Moribatake, M. Abe, E. Fujisaki, and Y. Nakayama, "Electronic cash scheme," in *Symposium on Cryptography and Information Security, Fukuoka, Japan*, January 1997, pp. SCIS97–3C.

[23] S. D'Amiano and G. D. Crescenzo, "Methodology for digital money based on general cryptographic tools," in *Proc. of Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT'94), Perugia, Italy, LNCS*, vol. 950. Springer-Verlag, May 1994, pp. 156–170.

[24] E. F. Brickell, P. Gemmell, and D. W. Kravitz, "Trustee-based tracing extensions to anonymous cash and the making of anonymous change," in *Proc. of the 6th Annual ACM-SIAM Symposium on Discrete Algorithms, San Francisco, California*. ACM, January 1995, pp. 457–466.

[25] J. Camenisch, U. M. Maurer, and M. Stadler, "Digital payment systems with passive anonymity-revoking trustees," in *Proc. of the 4th European Symposium on Research in Computer Security (ESORICS'96), Rome, Italy, LNCS*, vol. 1146. Springer-Verlag, September 1996, pp. 33–43.

[26] Y. Frankel, Y. Tsiounis, and M. Yung, "Indirect discourse proof: Achieving efficient fair off-line e-cash," in *Proc. of International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT'96), Kyongju, Korea, LNCS*, vol. 1163. Springer-Verlag, November 1996, pp. 286–300.

[27] K. Q. Nguyen, Y. Mu, and V. Varadharajan, "A new digital cash scheme based on blind nyberg-rueppel digital signature," in *Proc. of the 1st International Workshop on Information Security (ISW'97), Tatsunokuchi, Japan, LNCS*, vol. 1396. Springer-Verlag, September 1997, pp. 313–320.

[28] A. die Solages and J. Traoré, "An efficient fair off-line electronic cash system with extensions to checks and wallets with observers," in *Proc. of the 2nd International Conference on Financial Cryptography (FC'98), Anguilla, British West Indies, LNCS*, vol. 1465. Springer-Verlag, 1998, pp. 275–295.

[29] J. C. Pailles, "New protocols for electronic money," in *Proc. of Workshop on the Theory and Application of Cryptographic Techniques (AUSCRYPT'92), Gold Coast, Queensland, Australia, LNCS*, vol. 718. Springer-Verlag, December 1992, pp. 263–274.

[30] M. K. Franklin and M. Yung, "Secure and efficient off-line digital money (extended abstract)," in *Proc. of the 20th International Colloquium on Automata, Languages and Programming, (ICALP'93), Lund, Sweden, LNCS*, vol. 700. Springer-Verlag, July 1993, pp. 265–276.

[31] B. Schoenmakers, "An efficient electronic payment system withstanding parallel attacks," CWI, Tech. Rep. CS-R9522, March 1995.

[32] M. Jakobsson and M. Yung, "Revokable and versatile electronic money (extended abstract)," in *Proc. of the 3rd ACM Conference on Computer and Communications Security (CCS'96), New Delhi, India.* ACM, March 1996, pp. 76–87.

[33] M. K. Franklin and M. Yung, "Towards provably secure efficient electronic cash," Columbia University, Department of Computer Science, Tech. Rep. CUCS-018-92, April 1992.

[34] M. H. Au, W. Susilo, and Y. Mu, "Electronic cash with anonymous user suspension," in *Proc. of the 16th Australasian Conference on Information Security and Privacy (ACISP'11), Melbourne, Australia, LNCS*, vol. 6812. Springer-Verlag, July 2011, pp. 172–188.

[35] J. Camenisch, S. Hohenberger, and A. Lysyanskaya, "Compact e-cash," in *Proc. of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'05), Aarhus, Denmark, LNCS*, vol. 3494. Springer-Verlag, May 2005, pp. 302–321.

[36] M. H. Au, W. Susilo, and Y. Mu, "Practical anonymous divisible e-cash from bounded accumulators," in *Proc. of the 12th International Conference on Financial Cryptography and Data Security (FC'08), Cozumel, Mexico, LNCS*, vol. 5143. Springer-Verlag, January 2008, pp. 287–301.

[37] S. H. von Solms and D. Naccache, "On blind signatures and perfect crimes," *Computers & Security*, vol. 11, no. 6, pp. 581–583, October 1992.

[38] M. Abe, "A secure three-move blind signature scheme for polynomially many signatures," in *Proc. of International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'01), Innsbruck, Austria, LNCS*, vol. 2045. Springer-Verlag, May 2001, pp. 136–151.

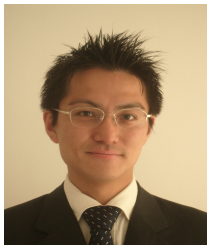
[39] V. Shoup, "Practical threshold signatures," in *Proc. of International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'00), Bruges, Belgium, LNCS*, vol. 1807. Springer-Verlag, May 2000, pp. 207–220.

[40] B. M. Bowen, S. Hershkop, A. D. Keromytis, and S. J. Stolfo, "Baiting inside attackers using decoy documents," in *Proc. of the 5th International ICST Conference on Security and Privacy in Communication Networks (SecureComm'09), Athens, Greece*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 19. Springer-Verlag, September 2009, pp. 51–70.

[41] J. Grier, "Detecting data theft using stochastic forensics," in *Proc. of the 11th Digital Forensic Research Workshop (DFRWS'11), New Orleans, USA*, ser. Digital Investigation, vol. 8. Elsevier, August 2011, pp. S71–S77.

[42] R. J. Perlman, C. Kaufman, and R. A. Perlner, "Privacy-preserving drm," in *Proc. of the 9th Symposium on Identity and Trust on the Internet (IDtrust'10), Gaithersburg, Maryland, USA*. ACM, April 2010, pp. 69–83.

Takashi Nishide received B.S. degree from the University of Tokyo in 1997, M.S. degree from the University of Southern California in 2003, and Dr.E. degree from the University of Electro-Communications in 2008. From 1997 to 2009, he had worked at Hitachi Software Engineering Co., Ltd. developing security products. Since 2009, he is an assistant professor in Kyushu University. His primary research is in the areas of cryptography and information security..



Shingo Miyazaki received B.S. degree and M.S. degree from Kyushu University in 1997 and 1999, respectively. He had worked at Toshiba Corporation from 1999 to 2002 and been seconded to YRP Ubiquitous Networking Laboratory from 2002 to 2007. Since 2007, he works at Toshiba Solutions Corporation. He is interested in information security and ubiquitous computing.

Kouichi Sakurai is Professor of Department of Computer Science and Communication Engineering, Kyushu University, Japan since 2002. He received B.E., M.E., and D.E. of Mathematics, Applied Mathematics, and Computer Science from Kyushu University in 1982, 1986, and 1993, respectively. He is interested in cryptography and information security. He is a member of IPSJ, IEEE and ACM.

A Remarks on Some E-Cash Systems

A.1 Brickell-Gemmel-Kravitz [24]

This is the first system that prevents blackmailing and money laundry. This system has two kinds of information related to customers. One is for double-spender-tracing: the bank can identify the identity of the customer that double-spends e-cash. The other is for one-payment-tracing: the bank and trustee can cooperate to de-anonymize a particular payment transaction and identity the customer. The classification here is based on the customer's secret and public information related to the former.

A.2 Ferguson [10]

Ferguson discusses the problem of bank's framing the honest customer as a double-spender. Though it is classified as Type I, the system that is resistant against framing is more secure against impersonation than other schemes in Type I. Therefore, it is of Type I^+, which is more secure than Type I.

As the first step of the presented solution, the secret key U of the customer is generated as $U =$ (his identity$\|$coin number) so that U can be different for all his e-cash. Second, each customer signs all data exchanged during the withdrawal protocol and sends them to the bank. When the bank claims the double spending of the customer, the bank computes U and extracts the coin number from U and identifies the transaction of the withdrawal protocol in which the e-cash was issued. The bank can use the customer's signature on the transaction data as evidence to accuse the customer. The bank does not know the customer's signing key, so the bank cannot forge a fact of double spending. However, the data exchanged during the withdrawal protocol need to be stored on both the customer and bank.

A.3 Fujisaki-Okamoto [17]

Fujisaki and Okamoto proposed two scheme that enhance the security of Type III. One scheme assumes an anonymous channel and separates the (multiple) authorities that keep the customer's ID-related information from the authority that manages the customer's public keys. Even if an adversary can obtain the list of public keys from the latter authority, the identity of the owner corresponding to the key is unknown. Obtaining the relationship between the key and the owner for impersonation requires the help from all the authorities.

The other scheme divides the customer's public key and the piece of the divided public key is escrowed to each authority with the customer's ID information. Since the information available from an authority is part of public key, the help from all the authorities is also required similarly to the above scheme. Therefore, the Fujisaki-Okamoto scheme is more resistant than other schemes in Type III in terms of the difficulty in relating the public key to the identity of the owner.

A.4 Jakobsson-Yung [32]

The classification of the scheme proposed by Jakobsson and Yung depends on the authentication method used in the withdrawal protocol, on which the original paper [32] gives no explicit description.

Suppose that an adversary can obtain the identity id of a customer stored in the database of a bank. When the customer is authenticated via the session key K_B sent to the bank in the withdrawal protocol, there can be several ways to generate K_B and it is related to the security. One way is that K_B is issued by the bank when the customer opens the account and is used for authenticating the customer. In the withdrawal protocol, the bank decrypts the key encrypted under the bank's public key and accepts the customer only when the decrypted key is equal to K_B agreed when the account is opened. In this case, an adversary can impersonate the customer only by obtaining the lists of K_B and id, which are stored in the database of the bank together. This approach makes the Jakobsson-Yung scheme belong to Type I in which obtaining the data stored in the bank allows the adversary to perform impersonation.

The other way is that with the public key of the customer, the bank authenticates the customer by verifying the signature in the challenge-response protocol. The scheme with this approach belongs to Type II, in which impersonation requires obtaining the secret key corresponding to the public key.

Another way is to use the Diffie-Hellman key K_B, as a session key, computed from the bank's secret key and the customer's public key certificate issued by CA. The bank can authenticate the customer by checking if a session key sent by the customer is the same as the Diffie-Hellman key. The scheme with this approach belongs to Type III because the adversary needs to obtain the corresponding certificate.

A.5 Pailles [29]

The bank checks whether the identity id_U of the customer is embedded in e-cash via the cut-and-choose method. id_U is known only to the bank and the customer. Then the double-spender can be identified from the extracted id_U. Although it is similar to other schemes in Type I because the bank stores id_U, this scheme compels each customer to sign all the data exchanged with the bank. The secret key for signing is known only to the customer and necessary for impersonation with a stolen id_U. Therefore, performing impersonation is more difficult than in other schemes of Type I.

A.6 Peterson-Poupard [21]

Each customer generates pseudonymous key pairs of the secret key S_U and public key P_U, and obtains the certificate of the pair issued by a trusted third party (TTP). Only the TTP knows the relationship between the customer and the pseudonym. The pseudonymous key pair is used for the challenge-response protocol in the payment. If the same pseudonym is used in many different payment transactions, the bank can revoke the anonymity of e-cash by checking the deposited e-cash when the relation between the customer and the pseudonym becomes clear. The unmasked pseudonym allows the bank to breach the privacy of the customer. In order to minimize the visible payment history by the revocation of a pseudonym and enhance the privacy of customers, each customer has many key pairs and makes payments using different pseudonyms. If the relationship between the customer and the pseudonym is made clear by the collusion of the bank and the shop, the customer makes payments with different key pairs by discarding the unmasked pseudonym.