A New Approach to Prevent Blackmailing in E-Cash[*]

Xiaofeng Chen[1], Fangguo Zhang[2] and Yumin Wang[1]

1 National Key Lab of ISN, Xidian University

Xi'an 710071 China

crazymount@hotmail.com

2 International Research center for Information Security (IRIS)

Information and Communications University (ICU)

58-4 Hwaam-dong, Yusong-Ku, Taejon, 305-732 KOREA

zhfg@icu.ac.kr

Abstract: Blackmailing may be the most serious drawback of the known electronic cash systems offering unconditional anonymity. Recently, D.Kugler proposed an on-line payment system without trusted party to prevent blackmailing based on the idea of *marking*. In this paper, some disadvantages of D.Kugler's scheme are analyzed and then a new online electronic cash scheme to prevent blackmailing is present by using group blind signature technique. In our scheme, the blackmailed cash was marked by an entity, called supervisor, therefore the bank can distinguish it from the valid cash. Also, we can modify our scheme to be offline so that it can used to decrease other crimes, e.g., money laundering, bribery etc. in electronic cash system.

Key words: Fair Electronic Cash; General Blackmailing; Group Blind Signature;

1 Introduction

Unconditionally anonymous electronic cash system [1] preserves the privacy of the users, while facilitates crimes such as money laundering, blackmailing and etc. V.Solms [2] firstly introduces the crime of blackmailing, and he presents an example of perfect crime. Blackmailing may be the most serious drawback of the known payment systems offering unconditional anonymity, for the bank cannot distinguish the blackmailed cash and the valid cash. Depending on the power of the blackmailer, blackmailing can be classified into the following cases [3]:

★ **Perfect crime**: The blackmailer contracts the victim via an anonymous channel and threatens him to withdraw a coin that is chosen and blinded by the blackmailer. The blackmailer communicates only with the victim but cannot observe the victim's

[*] Supported by National Science Foundation of China (60073052)

communication with the bank.

★ **Impersonation**: The blackmailer gains access to the victim’s bank account, e.g., he knows the victim’s secret shared with the bank, and pretends to be the victim to withdraw coins. The blackmailer communicates directly with the bank, but cannot observe the victim’s communication with the bank.

★ **Kidnapping**: The blackmailer has physical control over the blackmailed victim and withdraws the cash similar to the impersonation attack. The blackmailer communicates with the bank directly and prevents the victim from communication with the bank.

Stadler [4] introduces the concept of fair blind signature to prevent the misuse of unconditional anonymity by criminals, but he also points out that fair blind signature cannot solve the general problem of blackmailing: The blackmailer could force the bank and the trustee to use the truly blind signature protocol. It is still an open problem. Subsequently, a lot of electronic cash systems with revocable anonymity are proposed [5-9], that is, the trustee can help the bank to trace the dubious cash or users when needed. However, trustee-based system may suffer the problem of illegal tracing, i.e. the privacy of the honest users may be violated by the trustee.

To defeating blackmailing, it is required that the bank can distinguish the blackmailed cash with the valid one. Recently, D.Kugler [3] proposed an on-line payment system without trusted party to prevent blackmailing based on the idea of *marking*. The electronic cash mechanism has the following properties:

—Every blackmailed coin can be distinguished by a different mark.

—Only the bank can determine whether a coin is marked or not. For other entities marked coins are indistinguishable from unmarked coins.

—At withdrawal the bank must prove that a coin is unmarked, and the proof cannot be used to convince anybody except the owner of the bank account

—At deposit the bank can accept or reject the coins, depending on the choice of the blackmailed person.

—Marking cannot be used to trace honest users.

—All spent marked coins can efficiently be detected at deposit. This enables tracing of the blackmailer.

The idea of marking is excellent for it can distinguish the valid coins from the blackmailed coins. However, the idea is disabled in some cases. Also it has the following disadvantages, as mentioned in the paper:

—Blackmailing is not a frequent case compared with legal withdrawing the coins from the bank. So, the on-line system will be inefficient for practical use in most cases.

—The system cannot be applied to other crimes such as money laundering, illegal trade etc.

D.Kugler used the randomized blind undeniable signature scheme [10], which combines the

Okamoto-Schnorr blind signature scheme [11,12] with Chaum-van Antwerpen undeniable signature scheme [13], to construct his system. At the end of the withdrawal protocol, the bank must perform a confirmation protocol to prove the *validity* of an undeniable signature, which provides a proof to the honest user that the coin is unmarked. In case of blackmailing, a faked confirmation protocol is needed for the blackmailer to verify the *"validity"* of the coin. So, it is assumed that the victim can inform the bank of blackmailing in case of perfect crime and impersonation and the bank can always obtain the decryption key from the victim. However, these assumptions are impractical in real world, as discussed in details below:

Perfect crime

In the D.Kugler's scheme, valid coins are issued using a private key x while marked coins are issued using a different private key $SK_{U_M} = x_M$ to generate the undeniable signature. The bank cooperates with the victim to cheat the blackmailer if the bank knows the victim's decryption key. D.Kugler points out that the victim can himself to perform the confirmation protocol or tell his decryption key to the bank to cheat the blackmailer in the perfect crime.

But how would a "clever" blackmailer like to obey the rules of the bank? The blackmailer himself chooses secret $a, b \in_R Z/pZ$ and encrypts them with his private key. He then computes $f = w^a y^b \bmod p$ and threatens the bank to send him the value of $t = f^{x^{-1}} \bmod p$.

If the bank rejects the requirement of blackmailer, the victim will be killed. For the safety of the victim, the bank has no choice but to obey the "rules" of the blackmailer, just like the polices or FBI satisfy the claims of the robbers in the physical world. However, if the bank uses the marking key x_M instead of x, which means $w = \alpha^{x_M}$, the blackmailer will check $t \neq \alpha^a g_3^b \bmod p$. So the blackmailer can easily know whether the bank cheats him or not.

Impersonation

Han *et al* [14] points out the scheme of D.Kugler cannot solve the problem of *special impersonation*: if the blackmailer accidentally obtains the information to access the victim's bank account without threatening him, the victim cannot know even the fact that he is blackmailed.

Kidnapping:

When the blackmailer kidnapped a user, as D.Kugler mentioned in his paper, the user would need a covert channel to inform that he was kidnapped and tell the bank his decryption key for computing the secret parameters a and b. This is almost impossible for the physical world. A cruel blackmailer would try his best to prevent the victim from communicating with any other entities except himself. Also, the solution of using secure hardware for the authentication at the beginning of the withdrawal, just as [14] pointed out, can give the bank those information only with probability of 1/2. Once the victim cannot notify the bank about the blackmailing or inform the bank his decryption key, the blackmailer will succeed in withdrawing the cash without being detected forever.

Based on the property that the trace of congruent elements of XTR public key system is same, Han *et al* [14] present a scheme to defeating blackmailing with a probability. The scheme is practical but cannot solve the blackmailing entirely. In this paper, we present a new electronic cash scheme to prevent blackmailing by using the group blind signature technique and we need no impractical assumptions. ***Of course, we never think that the bank would work in tandem with blackmailer.*** To achieve our aims, an entity called supervisor is introduced, who forms a group with the bank. The supervisor would play the role of the bank when emergency such as blackmailing, that is, he would sign on the message of the criminals instead of the bank. From the properties of the group signature scheme, we can deduce that the criminals cannot distinguish the signature of the bank from that of the supervisor. However, the bank only accepts the cash signed by himself. So, when the blackmailed cash is deposited, the bank could distinguish it with the valid cash. The bank can accept or reject the coins, depending on the choice of the victim. We will prove: our scheme satisfies all advantages mentioned in D.Kugler's scheme even if the victim cannot communicate with the bank. Also we modify the scheme properly to make it an off-line system so that it also can be used to prevent other crimes related with anonymity.

The rest of the paper is organized as follows: In Section 2, we will present some preliminary works. Then we give the description of our fair electronic cash protocol and prove our scheme satisfies all advantages mentioned in D.Kugler's scheme even if the victim cannot communicate with the bank. In section 4, we analyze the security and efficiency of our proposed scheme. Finally, we give the conclusions.

2 Preliminary works

In this section, we will introduce the techniques of group signature and group blind signature, which we use to construct our electronic cash scheme against blackmailing.

2.1 Group signature

The concept of group signature is firstly introduced by Chaum [15]. In a group signature scheme, members of the given group can sign on behalf of the entire group. Everyone can verify the validity of the signature with group public key but no one except the group manager can determine which member signed the data. Recently, Camenisch [16] presented an efficient group signature for large group, which mainly uses the following technique:

Definition 1 Signature of knowledge of discrete logarithm

A pair of $(c,s) \in \{0,1\}^k \times Z_n^*$ satisfying $c = H(m \| y \| g \| g^s y^c)$ is a signature of knowledge of discrete logarithm of the element of $y \in G$ to the base g on the message m, and is denoted $SKREP[(\alpha,\beta): y = g^{\beta} h^{\alpha}](m)$.

Definition 2 Signature of knowledge of double discrete logarithm

Let $l \le k$ be a security parameter, an $l+1$ tuple $(c, s_1, \cdots, s_l) \in \{0,1\}^k \times Z^l$ satisfying the equation $c = H(m \| y \| g \| a \| t_1 \| \cdots \| t_l)$ with $t_i = \begin{cases} g^{a^{s_i}} & if\ c[i] = 0 \\ h^{a^{s_i}} & else \end{cases}$ and is denoted $SKLOGLOG[\alpha : y = g^{a^{\alpha}}](m)$.

Definition 3 Signature of knowledge of e-th root of the discrete logarithm

If an $l+1$ tuple $(c, s_1, \cdots, s_l) \in \{0,1\}^k \times Z^l$ satisfying the following equation: $c = H(m \| y \| g \| e \| t_1 \| \cdots \| t_l)$ with $t_i = \begin{cases} g^{s_i^e} & if\ c[i] = 0 \\ y^{s_i^e} & else \end{cases}$ and is denoted $SKROOTLOG[\alpha : y = g^{\alpha^e}](m)$.

Definition 4 Group signature scheme

Suppose Alice has been a member of a group. To sign a message m, she computes the following values:

--$\tilde{g} = g^r, r \in_R Z_n^*$; $\tilde{z} = \tilde{g}^y$;

--$V_1 = SKLOGLOG[\alpha : y = g^{a^{\alpha}}](m)$; $V_2 = SKROOTLOG[\beta : y = g^{\beta^e}](m)$;

So, the signature on the message m is $(\tilde{g}, \tilde{z}, V_1, V_2)$, which proves an entity indeed belongs to the group. Everyone can verify it by checking the correctness of V_1, V_2 with the group's public key.

2.2 Group blind signature

Lysyanskaya [17] presents an electronic cash scheme for distributed banks based on group blind signature technique, which combines the notions of blind signatures and group signatures. A group blind signature scheme satisfies the following properties:

—**Blindness of signature**: the signer is unable to view the messages he signs, while he can verify that he did indeed sign it. So the bank can determine whether a particular coin is signed by him or not and distinguish the marked coins from the valid coins.

—**Unforgeability**: only group members can sign on behalf of the entire group. So everyone can verify the invalid coins.

—**Undeniable signer identity**: the group manager can always establish the identity of the member who issued a particular signature.

—**Signer anonymity**: everyone except the group manager can never determine which member of the group issued the signature.

—**Unlinkability**: Two message-signature pairs where the signature was obtained from the same signer cannot be linked.

—**Security against framing attacks**: neither the group manager nor the members can sign on behalf of other group members.

With the notations of reference, the group blind signature on the message m consists of $(\hat{g}, \hat{z}, V_1, V_2)$ and can be verified by checking the correctness of V_1 and V_2, where $V_1 = SKLOGLOG_l[\alpha : \hat{z} = \hat{g}^{a^{\alpha}}](m), V_2 = SKROOTLOG_l[\beta : \hat{z}\hat{g} = \hat{g}^{\beta^{e}}](m)$. For details, see reference [17].

3 New electronic cash scheme to prevent blackmailing

In this section, we propose our electronic cash scheme to prevent general problem of blackmailing.

3.1 System parameters

RSA pubic key (n, e), the length of n is at least 1024 bits. A cyclic group $G =< g >$ of order n. We assume the discrete logarithm problem in G is hard. In particular, we can choose G to be a cyclic subgroup of Z_p^* where p is a prime and $n \mid p-1$. An element $a \in Z_p^*$ where a has large multiplicative order modulo all the prime factors of n. Upper bound λ for the size of secret key， a constant ε. The public key of the group is $\Omega = (n, e, a, G, g, \lambda, \varepsilon)$.

3.2 Main idea

A supervisor and a bank form a group and a trusted entity acts as the group manager. If a user, who shares a secret with the bank, wants to withdraw electronic cash from his account, and he creates an electronic coin m. The bank applies a group blind signature protocol to m and decreases appropriate amount from the user’s account. Everyone including the vendor can verify the validity of signature with public key of the group. The vendor then sends the coins to the bank, and the bank checks the signature is indeed his and accepts the coin.

If a criminal, Bob, kidnaps a baby and menaces the bank to sign on the “coin” m. The supervisor then applies a group blind signature protocol to m instead of the bank but Bob cannot detect this. When the vendor deposits the marked cash in the bank, the bank can verify the cash is not signed by himself. So all spent marked coins can efficiently be detected at deposit. Accepting or rejecting the coin depends on the choice of the blackmailed user.

3.3 How to notify the bank

It is a crucial problem for the blackmailed user to notify the bank the blackmailing without being detected by criminals. It is a dangerous and difficult task because the criminal will try his best to prevent the victim to communicate with other entities except him.

When a user opens an account in the bank, he shares a secret with the bank to authenticate his identity for future withdrawal. Suppose the shared secret is $S = s_1 \| s_2$, where "||" stand for concatenation and an agreed symmetric algorithm (e.g. AES) with key K is $E_K()$.

When the user wants to withdraw a coin from his account, the bank firstly sends him two random messages m_1, m_2. The user then computes ($E_{s_1}(m_1), E_{s_2}(m_2)$) and sends the pair to the bank. The bank uses the agreed symmetric algorithm with key s_1, s_2 respectively to decrypt the pair ($E_{s_1}(m_1), E_{s_2}(m_2)$). Suppose the decrypted messages are (n_1, n_2). If $n_1 \neq m_1$, the bank rejects to serve for the user. If $n_1 = m_1$ and $n_2 = m_2$, the bank knows the user is the owner of the account. If $n_1 = m_1$ but $n_2 \neq m_2$, the bank will deduce the owner of the account is controlled by a blackmailer.

So, when the blackmailer communicates directly with the bank to withdraw the coins, the blackmailed user makes the criminal himself notify the bank the blackmailing.

Maybe someone think our assumption is not strong enough, because the blackmailer is able to force the victim to tell him the true secret and get unmarked coins. In fact, the blackmailer cannot distinguish the true secret with the false one, and he just uses the "secret" to withdraw the coins from the blackmailed user's account. If the bank (in fact, the supervisor) signs to the coins, he thinks the "secret" is true. Furthermore, he cannot distinguish the signature of the bank from that of the supervisor. So, the blackmailer gets the marked coins unconsciously.

3.4 Our fair electronic cash scheme

Our scheme mainly includes the following protocols:

3.4.1 Setup of the groups

Suppose the group public keys are $\Omega = (n, e, a, G, g, \lambda, \varepsilon)$. If an entity wants to join the group, he picks a secret key $x \in_R \{0, 1, \cdots, 2^\lambda - 1\}$ and computes $y = a^x \bmod n$. His membership key $z = g^y$, and he commits himself to y. He then sends y, z to the group manager and that he knows the discrete logarithm of y to the base a. When the group manager is convinced that the entity knows the logarithm, he returns the member certificate $v = (y+1)^{1/e} \bmod n$.

So do the bank and the supervisor to join the group and get their member certificate.

3.4.2 Withdrawal of the cash

If a legitimate user wants to withdraw an electronic coin m, the bank firstly verifies the validity of shared secret and then applies *the group blind signature protocol* to m. Suppose the resulting signature is $(\hat{g}, \hat{z}, V_1, V_2)$ and the user verifies its validity by checking correctness of V_1 and V_2.

Suppose a blackmailer kidnapped a user and forced him to tell his secret shared with the bank. The user then told the blackmailer the secret is $S' = s_1 \| s_2'$, while his true secret is $S = s_1 \| s_2$. So the bank will know a blackmailer controlled the user and then the supervisor applies *the group blind signature protocol* to the coin m created by the criminals. The blackmailer can verify the validity of the signature but cannot detect the coin was marked by the supervisor.

3.4.3 Purchasing the goods

The vendor cannot check the validity of the coin either, and he immediately deposits the coins at the bank (in section 3.4, we will discuss the case of that the vendor need not to deposit the coin immediately). The bank first verifies the validity of the signature, and then tests whether $\hat{z} = \hat{g}^{y_B}$ (y_B is the membership key of the bank). If the test fails but the signature is valid, the bank knows it is a marked coin. Depending on the choice of the blackmailed user, the coin can be accepted or rejected.

If the test succeeds and the coin was not deposited before, the bank accepts the coin. Then the vendor sends the goods to the buyer.

3.5 Make our scheme off-line

It is a drawback that the above system is an online system, which is much inefficient for most of users. In the following we will modify it to be an offline system.

Suppose all spenders who open an account form the second group and a trusted party is the group's manager. Suppose the group public keys are $\Omega' = (n, e, a', G, g', \lambda, \varepsilon)$.

The withdrawal protocol is same as above. In the purchasing protocol, the vendor firstly verifies the validity of *group blind signature* $(\hat{g}, \hat{z}, V_1, V_2)$ with public key Ω, and the user proves that he belongs to the second group as follows:

The user computes $m^{'} = H(\hat{g} \,||\, \hat{z} \,||\, V_1 \,||\, V_2)$, here H is a collision-free function and || denotes catenations. He applies *the group signature protocol* to $m^{'}$, and the vendor can verify the validity of the signature $(\tilde{g}, \tilde{z}, V_1^*, V_2^*)$ with the public key Ω'. If both the signatures are valid, he sends his goods to the user. Otherwise, he rejects the cash.

When the vendor wants to deposit the cash (he need not to deposit the coins immediately during the period of sale), the bank can distinguish the marked cash from the valid cash. Also the scheme can be used to solve other anonymity related problems such as money laundering, illegal purchases etc with the help of the second group manager.

4 Security analyze

- ***Unforgability of Coins*** Every blackmailed coin can be distinguished by a different mark. The supervisor can join the group repeatedly with different secret keys. Another solution is to use distributed supervisors. A dishonest supervisor cannot forge the coin. When a blackmailing happens, the bank notifies a supervisor to sign instead of him and gives him a proof. After a marked coin was detected, the group manager can find out which supervisor issued the signature. If the supervisor was not notified to mark a coin by the bank, it can be deduced the supervisor forge the coin. Also when different coins with the same marking were detected, the corresponding supervisor must be responsible for his dishonest deeds.

- ***Undetectability of Marking*** From the property of group signature, we can deduce that only the bank can detect whether a coin is marked or not. For other entities marked coins are indistinguishable from unmarked coins.

- ***Tracing of the blackmailer*** All spent marked coins can efficiently be detected at deposit. This enables tracing of the blackmailer. At deposit the bank can accept or reject the coins, depending on the choice of the blackmailed person. When the victim is set free, he can request the bank to announce the invalidity of all unspent marked coins. The blackmailed user publics his membership key of the second group, then the vendor will reject the corresponding marked coins. So these unspent coins can be refunded to the user. When a blackmailer is caught, the corresponding mark key is published and all coins with this mark are always rejected by the vendor or the bank.

- ***Unconditional Anonymity for Honest Users*** If the supervisors will not work in tandem with the bank, marking cannot be used to trace the honest users. Therefore, our scheme provides unconditional anonymity for the legal and honest users if the manager of the second group is honest. It may be regarded as a solution to the problem of ***general blackmailing***.

- ***Practical Assumption*** Our scheme dose not rely on any secure hardware and cover channel for the kidnapping scenario. It is a reasonable assumption that the bank will not collude with the supervisors, just as we believe that the bank will collude with the trustee in fair electronic cash systems.

To sum up, our scheme satisfies all advantages mentioned in D.Kugler’s scheme even if the victim cannot communicate with the bank.

Also, our scheme solved two open problems mentioned in D.Kugler’s scheme: Firstly, it can be extended to other blackmailing scenario, e.g. the bank is blackmailed. If the blackmailer threatens the bank to reveal his signing key to him, the bank just sends the *marking* key of the supervisor to the blackmailer and he cannot distinguish it. So, any coins signed by the marking key will be detected by the bank. Secondly, we find a solution for kidnapping scenario that does not rely on any secure hardware.

5 Efficiency analyze

To prevent the bank to trace his coins withdrawn previously, the user should have at least two membership keys of the second group. If a particular membership key is used to deal with the emergent cases such as blackmailing, the privacy of the user will remain untouched even the key is public. The group signature scheme of Camenisch is suit for a large group, so our scheme is much efficient even though the user joins the group repeatedly. Furthermore, we can use group blind signature protocol based on elliptic curve to construct our scheme, so that the amount of the computation and the data need to be transferred can be decreased greatly. For details, see reference [18].

6 Conclusions

In this paper, a new online electronic cash scheme to prevent blackmailing is present by using group blind signature technique. The blackmailed cash was *marked* by an entity, called supervisor, so that the bank can distinguish it from the valid cash. Our scheme not only has all the advantages of D.Kugler’s scheme, but also overcomes its some drawbacks such as inefficiency and impractical assumptions.

However, our scheme relies on the trusted third parties, and it may suffer from attack of illegal tracing, which maybe possible in systems with revocable anonymity [5--9]. It was left as an open problem.

References

[1] D. Chaum, “Blind Signature for Untraceable Payments”, **EUROCRYPT’82**, Plenum Press, pp.199—203, 1983.

[2] B.von Solms, D. Naccache, “On blind signatures and perfect crimes”, **Computers and Security**, 11(6), pp. 581—583, 1992.

[3] D.Kugler, H. Vogt, “Marking: A Privacy Protecting Approach Against Blackmailing”, **PKC’01,** LNCS 1992, Springer-Verlag, pp.137—152, 2001.

[4] M. Stadler, J.M.Piveteau and Jan.Camenisch, “Fair blind signatures”, **EUROCRYPT’95**,

LNCS 921, Springer-Verlag, pp.209—219, 1995.

[5] E. Brickell, P.Gemmell and D. Kravitz, “Trustee—based Tracing Extension to Anonymous Cash and the Marking of Anonymous Change”, **Proc. 6-th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)**, pp. 457—466, 1995.

[6] J.Camenisch, U. Maurer, M. Stadle, “Digital payment systems with passive anonymity-revoking trustees, **Computer Security Esorics’96**, LNCS 1146, Springer-Verlag, pp. 33—43, 1996.

[7] A. Juels, “Trustee Tokens: Simple and Practical Anonymous Digital Coin Tracing”, **Financial Cryptography '99**, LNCS 1648, Springer-Verlag, pp. 33—43, 1999.

[8] T. Sander, A. Ta—Shma, “Auditable, Anonymous Electronic Cash ”, **CRYPTO '99**, LNCS 1648, Springer-Verlag, pp.555—572, 1999.

[9] M. Jackbosson, M. Yung, “Revokable and versatile electronic money”, **In 3rd ACM Conference on Computer and Communications security**, ACM press, India, pp. 76—87, 1996.

[10] D. Chaum, “Zero-knowledge undeniable signature”，**EUROCRYPT’90**, LNCS 473, Springer-Verlag, pp.458—464, 1990.

[11] T.Okamato, “Provably secure and practical identification schemes and corresponding signature schemes”, **CRYPTO'92,** LNCS 740, Springer-Verlag, pp. 31—53, 1992.

[12] D. Pointcheval and J.Sten, “Provably secure blind signature schemes”, **ASIACRYPT’96**, LNCS 1163, Springer-Verlag, pp.252—265, 1996.

[13] D. Chaum and H.van Antwerpen, “Undeniable Signatures”, **CRYPTO'89**, LNCS 435, Springer-Verlag, pp.212—216, 1991.

[14] D. Han *et al*, “A Practical Approach Defeating Blackmailing,”**ACISP’02**, Springer-Verlag, pp.464-481, 2002.

[15] D.Chaum and E.van Heijst, **“**Group Signatures”, **EUROCRYPT’91,** LNCS 547, Springer-Verlag, pp.257—265, 1991.

[16] J.Camenisch and M.Stadler, “Efficient group signature schemes for large groups”, **CRYPTO'97,** LNCS 1294, Springer-Verlag, pp. 410—424, 1997.

[17] A.Lysyanskays, Z.Ramzan, “Group blind signatures: A scalable solution to electronic cash”, **Financial Cryptography '98**, LNCS1465, Springer-Verlag, pp.184—197, 1998.

[18] F.G. Zhang *et al*, “Fair electronic cash system with multiple banks”, **In 16th Annual Working Conference on Information security**, Kluwer Academic publishers, pp.461—470, 2000.